

DECOMPOSITIONS OF CONGRUENCE SUBGROUPS OF CHEVALLEY GROUPS

SERGEY SINCHUK AND ANDREI SMOLENSKY

ABSTRACT. We formulate and prove relative versions of several classical decompositions known in the theory of Chevalley groups over commutative rings. As an application we obtain upper estimates for the width of principal congruence subgroups in terms of several families of generators. Some of our results are new even in the absolute case and were previously studied only for groups over finite fields.

1. INTRODUCTION

Let $G(\Phi, R)$ be the simply-connected Chevalley group of type Φ over an arbitrary commutative ring R and let $E(\Phi, R)$ be its *elementary subgroup*, i. e. the subgroup generated by the elementary root unipotents $x_\alpha(\xi)$, $\alpha \in \Phi$, $\xi \in R$, see [18, 19, 32]. For an ideal $I \trianglelefteq R$ we denote by $G(\Phi, R, I)$ the *relative Chevalley group* (alias the *principal congruence subgroup*) of level I , i. e. the kernel of the map $G(\Phi, R) \rightarrow G(\Phi, R/I)$ induced by the canonical projection $R \rightarrow R/I$.

We will also use the notion of the *relative elementary Chevalley subgroup* $E(\Phi, R, I) \leq G(\Phi, R, I)$. Recall that $E(\Phi, R, I)$ is defined to be the normal closure in $E(\Phi, R)$ of the subgroup generated by the set $\mathcal{X} = \{x_\alpha(\xi) \mid \alpha \in \Phi, \xi \in I\}$.

Set $z_\alpha(s, \xi) = x_\alpha(s)^{x^{-\alpha}(\xi)}$, $s \in I$, $\xi \in R$. It is a classical result of J. Tits and L. Vaserstein (see [24], [26, Theorem 2]) that the relative elementary subgroup $E(\Phi, R, I)$ is generated by the set of elements $\mathcal{Z}(\Phi)$.

Here for a subset of roots $S \subseteq \Phi$ we denote by $\mathcal{Z}(S)$ the set

$$\mathcal{Z}(S) = \mathcal{X} \cup \{z_\alpha(s, \xi) \mid s \in I, \xi \in R, \alpha \in S\}.$$

The following recent result of A. Stepanov served as a starting point for the present paper. The notation for the subgroups involved in the statements of the results below is introduced properly in section 2.

Proposition 1.1 ([19, Theorem 3.4]). *Let Φ be a reduced irreducible root system of rank ≥ 2 , let $S \subset \Phi$ be an arbitrary parabolic subset of roots, and Σ_S be the special part of S . The relative elementary subgroup $E(\Phi, R, I)$ is generated as an abstract group by the set $\mathcal{Z}(\Sigma_S)$.*

The purpose of this paper is two-fold. First, we obtain relative analogues of several classical parabolic factorizations of Chevalley groups such as the Gauss, Bass—Kolster and

Date: November 11, 2015.

Key words and phrases. parabolic decomposition, bounded generation, SL_2 -factorization, subsystem factorization, product decomposition. *Mathematical Subject Classification (2010):* 20G40, 20G35, 19B14.

Authors of the present paper acknowledge the financial support from Russian Science Foundation grant 14-11-00297.

Dennis—Vaserstein decompositions. Then we apply these factorizations to the study of various bounded generation properties of Chevalley groups over rings.

Our first result is a relative version of the Gauss decomposition formulated in terms of the *stable rank* of the ideal I (see section 3 for the definition)

Theorem 1. *Let Φ be a root system, let I be an ideal of an arbitrary commutative ring R , and assume that $\text{sr}(I) = 1$. Then the relative elementary Chevalley group $E(\Phi, R, I)$ admits the following decomposition:*

$$E(\Phi, R, I) = H(\Phi, R, I) \cdot U(\Phi, I) \cdot U(\Phi^-, I) \cdot U(\Phi, I).$$

In the special case when I is contained in the Jacobson radical of R , Theorem 1 boils down to [1, Proposition 2.3]. We also note that the absolute case (i. e. $I = R$) of the theorem was treated by the second named author in [17].

The next main result is the relative Dennis—Vaserstein decomposition, which holds for a broader class of rings as compared to Theorem 1.

Theorem 2. *Let $\Phi \neq E_8$ be a reduced irreducible root system of rank $\ell \geq 2$ and let $\{r, s\}$ be a pair of distinct terminal vertices of the Dynkin diagram of Φ . Denote the distance between r and s by d . Assume that Φ , I and $\{r, s\}$ satisfy either of the following assumptions:*

- (1) $\text{sr}(I) \leq d$ for classical Φ ,
- (2) $\text{sr}(I) \leq d$ for $\Phi = E_\ell$ with $\{r, s\} = \{2, \ell\}$,
- (3) $\text{asr}(I) \leq d$ for $\Phi = E_\ell$ with $\{r, s\} = \{1, \ell\}$,
- (4) $\text{asr}(I) \leq d$ for $\Phi = F_4$.

Then $E(\Phi, R, I) = \text{EP}_r(R, I) \cdot U(\Sigma_r^- \cap \Sigma_s^-, I) \cdot \text{EP}_s(R, I)$.

Even in the special case $I = R$ the above theorem contains several new cases as compared to [18, Theorems 2.5 and 4.1]. The term “Dennis—Vaserstein decomposition” is due to A. Suslin and M. Tulenbaev (cf. [20, Lemma 2.1]).

The condition $\text{asr}(I) \leq d$ used in the statement of Theorem 2 is a relative version of the *absolute stable range* condition of D. Estes and J. Ohm, which depends only on the ideal I (see section 3.2).

Let G be an abstract group with a generating set $X \subset G$. We denote by $W(G, X)$ the *width of G with respect to X* , i. e. the smallest natural number N such that every element of G is a product of at most N elements of X .

Our first application of the parabolic factorizations is the following theorem, which gives an upper bound on the width of $E(\Phi, R)$ in terms of Tits generators. Thus, it is a quantitative analogue of Proposition 1.1 and a relative analogue of the results of [22, 33, 34].

Theorem 3. *Let I be an ideal of a commutative ring R .*

- (1) *If $R = \mathcal{O}_S$ is a Dedekind ring of arithmetic type possessing a real embedding and Φ is classical of rank ≥ 2 , then $W(G(\Phi, R, I), \mathcal{Z}(\Sigma_\ell^-))$ is finite;*
- (2) *If $\text{sr}(I) = 1$ and Φ is an arbitrary irreducible root system, then*

$$W(E(\Phi, R, I), \mathcal{Z}(\Pi)) \leq 3|\Phi^+| + 2\text{rk}(\Phi) - 1;$$

- (3) If $R = \mathbb{Z}[1/p]$ for some prime number p , then under the assumption of the Generalized Riemann Hypothesis one has

$$\begin{aligned} W(E(\Phi, R, I), \mathcal{Z}(\Sigma_\ell^-)) &\leq 3|\Phi^+| + 2\operatorname{rk}(\Phi) + 1 \quad \text{if } \Phi = A_\ell, C_\ell, \\ W(E(\Phi, R, I), \mathcal{Z}(\Sigma_\ell^-)) &\leq 4|\Phi^+| + \operatorname{rk}(\Phi) + 1 \quad \text{if } \Phi = B_\ell, D_\ell. \end{aligned}$$

The first assertion of the above theorem is essentially a reformulation of a previously known result of O. Tavgen (see [23], cf. [14]), while for the second and the third assertion we give a direct proof. Compare Theorem 3 with a recent result of U. Hadad and D. W. Morris [8, Theorem 1.6] which asserts that $W(\operatorname{SL}(n, \mathbb{Z}, I), \mathcal{Z}(\Pi))$ is finite for any ideal $I \leq \mathbb{Z}$ and $n \geq 3$.

Another application of the parabolic factorizations developed in the present paper is the subsystem factorization in terms of subgroups of type A_1 . The case of a finite field $R = F$ was studied by M. Liebeck, N. Nikolov and A. Shalev in [11]. More precisely, for an untwisted Chevalley group it has been proved that $G(\Phi, F)$ is a product of at most $N = 5|\Phi^+|$ copies of $\operatorname{SL}(2, F)$.

In [31] N. Vavilov and E. Kovach noted that the Bruhat decomposition immediately implies a bound of $N = 3|\Phi^+|$ factors for an arbitrary field F . In fact, in the assumptions of Theorem 1 one can immediately obtain the decomposition of $E(\Phi, R, I)$ with $3|\Phi^+|$ factors of type A_1 . Our next result further extends this to an even larger class of rings (which, for example, includes the ideals of all Dedekind rings).

Theorem 4. *Let $I \trianglelefteq R$ be an ideal, Φ be an irreducible classical root system satisfying one of the following assumptions.*

$$\begin{aligned} \Phi = A_\ell, \quad \operatorname{sr}(I) &\leq 2, \quad N = 3|\Phi^+| - \operatorname{rk}(\Phi) - 1; \\ \Phi = C_\ell, \quad \operatorname{sr}(I) &\leq 3, \quad N = 3|\Phi^+| - 2; \\ \Phi = B_\ell, D_\ell, \quad \operatorname{asr}(I) &\leq 2, \quad N = 4|\Phi^+| - 3\operatorname{rk}(\Phi). \end{aligned}$$

Then the principal congruence subgroup $G(\Phi, R, I)$ can be presented as a product of at most N copies of its (regularly embedded) subgroups isomorphic to $\operatorname{SL}_2(R, I)$.

Yet another application of the parabolic factorizations concerns the product decompositions of Chevalley groups formulated in terms of subgroups of type A_ℓ of submaximal rank. Recall that in [15] N. Nikolov proves the following result.

Theorem. *Let G be a classical Chevalley group (of normal or twisted type) of rank ℓ over a finite field F . Then G can be presented as a product of at most 200 conjugates of its subgroups of type $A_{\ell-1}$.*

It is classically known that over an arbitrary field F the group $\operatorname{SL}_{n+1}(F)$, $n \geq 3$ is a product of at most 4 subgroups of type $\operatorname{SL}(n, F)$. On the other hand, one immediately obtains from Theorem 2 and surjective stability for linear K_1 -functor that $\operatorname{SL}_{n+1}(R, I)$ factors into a product of at most 5 subgroups of type $\operatorname{SL}_n(R, I)$ for any ideal I satisfying $\operatorname{sr}(I) \leq n - 1$.

Applying Theorem 2 and proving a more accurate version of [15, Proposition 1] in the special case $\Phi = D_\ell$, we obtain the following result.

Theorem 5. *Assume that $\operatorname{sr}(I) \leq 2$. Then the group $\operatorname{Epin}_{2\ell}(R, I) = E(D_\ell, R, I)$ is a product of at most 9 conjugates of its (regularly embedded) subgroups of type $A_{\ell-1}$.*

The rest of the article is organized as follows. In sections 2–3 we introduce the principal notation and prove some basic facts pertaining to Chevalley groups over rings and the stability conditions. In section 4 we construct various parabolic factorizations and thus prove Theorems 1, 2 and 4. Finally, we treat the bounded generation and the product decompositions separately in section 5, where Theorems 3 and 5 are proved.

2. PRELIMINARIES

For any collection of subsets H_1, \dots, H_n of a group G we denote by $H_1 \dots H_n$ their Minkowski set-product, i.e. the set consisting of arbitrary products $h_1 \dots h_n$ of elements $h_i \in H_i$. In particular, the equality $G = H_1 \dots H_n$ means that every element $g \in G$ can be presented as a product $h_1 \dots h_n$, where $h_i \in H_i$ for each i .

2.1. Root systems. Let Φ be a reduced irreducible root system of rank ℓ with a fixed basis of fundamental roots $\Pi = \{\alpha_1, \dots, \alpha_\ell\}$. We use the conventional numbering of basis vectors of Π which follows Bourbaki (see [16, Table 1]). Denote by Φ^+ and Φ^- the subsets of positive and negative roots with respect to Π . Let α_{\max} denote the maximal root of Φ . For a root $\alpha \in \Phi$ we denote by $m_i(\alpha)$ the i -th coefficient in the expansion of α with respect to Π , i.e. $\alpha = \sum_{i=1}^n m_i(\alpha) \alpha_i$.

A proper closed subset of roots $S \subseteq \Phi$ is called *parabolic* (resp. *reductive*, resp. *special*) if $\Phi = S \cup -S$ (resp. $S = -S$, resp. $S \cap -S = \emptyset$). Any parabolic subset $S \subseteq \Phi$ can be decomposed into the disjoint union of its *reductive* and *special* parts, i.e. $S = \Sigma_S \sqcup \Delta_S$, where $\Sigma_S \cap (-\Sigma_S) = \emptyset$, $\Delta_S = -\Delta_S$.

We denote by (α, β) the scalar product of roots and by $\langle \alpha, \beta \rangle$ the integer $2(\alpha, \beta)/(\beta, \beta)$. Let $\varpi_1, \dots, \varpi_\ell$ be the *fundamental weights* of Φ , i.e. vectors defined by $\langle \varpi_i, \alpha_j^\vee \rangle = \delta_{i,j}$, where $\alpha^\vee = \frac{\alpha}{2(\alpha, \alpha)}$.

Denote by $W(\Phi)$ the subgroup of isometries of Φ generated by all simple reflections σ_α , $\alpha \in \Phi$. Recall that a simple reflection is defined by $\sigma_\alpha(\beta) = \beta - \langle \beta, \alpha \rangle \cdot \alpha$. For a reductive subset $\Delta \subseteq \Phi$ denote by $W(\Delta)$ the subgroup of $W(\Phi)$ generated by σ_α for $\alpha \in \Delta$.

Let $J \subseteq \Pi$ be a subset of fundamental roots. For a root $\beta = \sum m_i(\beta) \alpha_i \in \Phi$ define J -*shape* of β (denoted $\text{shape}(J, \beta)$) as $\sum_{i \in J} m_i(\beta) \alpha_i$. Set

$$\begin{aligned} \Delta_J &= \{\alpha \in \Phi \mid \text{shape}(J, \alpha) = 0\}, \\ \Sigma_J^\pm &= \{\alpha \in \Phi \mid \text{shape}(J, \alpha) \in \mathbb{Z}_{\geq 0} \Phi^\pm\}, \\ S_J^\pm &= \Delta_J \sqcup \Sigma_J^\pm. \end{aligned}$$

Clearly, Δ_J is a reductive subset, while S_J^\pm and Σ_J^\pm are parabolic and special subsets, respectively. For two disjoint subsets $I, J \subseteq \Pi$ one has

$$\Sigma_{I \cup J}^\pm = \Sigma_I^\pm \cup \Sigma_J^\pm, \quad \Delta_{I \cup J} = \Delta_I \cap \Delta_J.$$

We tend to omit curly braces in the above notations in the case when J is a one or two element set, e.g., $\Delta_k = \Delta_{\{k\}}$ and $\Sigma_{i,j}^\pm = \Sigma_{\{i,j\}}^\pm$, etc.

Lemma 2.1 ([2, Lemma 1]). *Let $\alpha, \beta \in \Sigma_J^\pm$ be two roots having the same length such that $\text{shape}(J, \alpha) = \text{shape}(J, \beta) \neq 0$. Then α and β are conjugate under the action of $W(\Delta_J)$.*

2.2. Chevalley groups and their elementary subgroups. Our exposition of Chevalley groups is standard and follows [18, 19, 21, 26, 32]. We denote by $G(\Phi, R)$ the simply-connected Chevalley group of type Φ over an arbitrary commutative ring R . For example, for each of the four classical series $\Phi = A_\ell, B_\ell, C_\ell, D_\ell$ the group $G(\Phi, R)$ equals $SL(\ell + 1, R)$, $Spin(2\ell + 1, R)$, $Sp(2\ell, R)$, $Spin(2\ell, R)$, respectively.

Notice that from the uniqueness theorem of M. Demazure (see [4, Corollaire 5.2]) it follows that the exceptional isomorphisms of small-rank groups (which are well-known in the theory of groups over fields) remain valid for Chevalley groups over arbitrary commutative rings. In particular, there are isomorphisms of groups $Spin(3, R) \cong SL(2, R)$, $Spin(5, R) \cong Sp(4, R)$, $Spin(6, R) \cong SL(4, R)$, $SL(2, R) \cong Sp(2, R)$.

Recall from [18, 32] that for $\alpha \in \Phi$, $\xi \in R$ one can define certain elements $x_\alpha(\xi)$ of $G_{sc}(\Phi, R)$, called the *elementary root unipotents*. These elements satisfy the well-known Steinberg relations:

$$(2.1) \quad x_\alpha(s)x_\alpha(t) = x_\alpha(s+t),$$

$$(2.2) \quad [x_\alpha(s), x_\beta(t)] = \prod x_{i\alpha+j\beta} (N_{\alpha\beta ij} s^i t^j), \quad \alpha \neq -\beta, \quad N_{\alpha\beta ij} \in \mathbb{Z}.$$

The indices i, j in the above formula range over all positive integers such that $i\alpha + j\beta \in \Phi$. The integers $N_{\alpha\beta ij}$ are called the *structure constants* of the Chevalley group $G(\Phi, R)$ and depend only on Φ . We refer the reader to [32, §14] for basic properties of the structure constants.

For an additive subset $I \subseteq R$ we denote by $X_\alpha(I)$ the corresponding *root subgroup* of level I , i.e. the subgroup consisting of all elementary root unipotents $x_\alpha(\xi)$, $\xi \in I$.

The subgroup $E(\Phi, R)$, generated by all $X_\alpha(R)$, $\alpha \in \Phi$ is called the *elementary subgroup* of the Chevalley group $G_{sc}(\Phi, R)$.

For $\varepsilon \in R^*$ set $w_\alpha(\varepsilon) = x_\alpha(\varepsilon)x_{-\alpha}(-\varepsilon^{-1})x_\alpha(\varepsilon)$. If $\text{rk}(\Phi) \geq 2$ the following relation is a consequence of (2.1)–(2.2):

$$(2.3) \quad w_\alpha(\varepsilon)x_\beta(\xi)w_\alpha(\varepsilon)^{-1} = x_{\sigma_{\alpha\beta}}(\eta_{\alpha,\beta} \cdot \varepsilon^{-\langle \beta, \alpha \rangle} \xi), \quad \varepsilon \in R^*, \quad \xi \in R.$$

where $\eta_{\alpha,\beta} = \pm 1$. The coefficients $\eta_{\alpha,\beta}$ can be expressed through the structure constants (see [32, §13]). For a reductive subset $\Delta \subseteq \Phi$ denote by $\widetilde{W}(\Delta)$ the *extended Weyl group*, i.e. the subgroup of $E(\Phi, R)$ generated by all $w_\alpha(1)$, $\alpha \in \Delta$.

Lemma 2.2. *Let Φ be an irreducible root system and let I be an ideal of R .*

- (1) *For every two roots $\alpha, \beta \in \Phi$ of the same length there exists $w \in \widetilde{W}(\Phi)$ such that $X_\alpha(I)^w = X_\beta(I)$.*
- (2) *The elementary group $E(\Phi, R)$ is generated as an abstract group by the root subgroups $X_\alpha(R)$, $\alpha \in \Pi \cup -\Pi$.*
- (3) *Assume that $\alpha_s \in \Pi$ is a fundamental root of Φ such that $m_s(\alpha_{\max}) = 1$. Then for $\alpha, \beta \in \Sigma_s^\pm$ of the same length there exists $w \in \widetilde{W}(\Delta_s)$ such that $X_\alpha(I)^w = X_\beta(I)$.*

Proof. The first statement of the lemma follows from identity (2.3) and the well-known fact that the Weyl group $W(\Phi)$ acts transitively on the set of roots of the same length.

The same argument combined with Lemma 2.1 also proves the third statement. Indeed, by our assumption all roots of the same length lying in Σ_s have the same s -shape.

To prove the second assertion notice that the subgroup $\langle X_\alpha(R) \mid \alpha \in \Pi \cup -\Pi \rangle$ contains $\widetilde{W}(\Phi)$ and therefore contains all other root subgroups $X_\alpha(R)$, $\alpha \in \Phi$. \square

Define the semisimple root elements $h_\alpha(\varepsilon)$, $\alpha \in \Phi$, $\varepsilon \in R^*$ as $h_\alpha(\varepsilon) = w_\alpha(\varepsilon)w_\alpha(-1)$. The elements $h_\alpha(\varepsilon)$ satisfy the following relations:

$$(2.4) \quad [h_\alpha(\varepsilon_1), h_\beta(\varepsilon_2)] = 1, \quad \alpha, \beta \in \Phi, \varepsilon_1, \varepsilon_2 \in R^*;$$

$$(2.5) \quad h_\alpha(\varepsilon_1\varepsilon_2) = h_\alpha(\varepsilon_1)h_\alpha(\varepsilon_2), \quad \alpha \in \Phi, \varepsilon_1, \varepsilon_2 \in R^*;$$

$$(2.6) \quad h_\alpha(\varepsilon)x_\beta(\xi)h_\alpha(\varepsilon)^{-1} = x_\beta(\varepsilon^{\langle\beta, \alpha\rangle}\xi), \quad \alpha, \beta \in \Phi, \varepsilon \in R^*, \xi \in R.$$

2.3. Representations of Chevalley groups. Our notation and terminology pertaining to the representations of Chevalley groups follows [16, § 1.4] and [13, § I.2]) Let π be an irreducible representation of $G(\Phi, R)$ acting on a free R -module V . We denote by $\Lambda = \Lambda(\pi)$ the set of weights of π and by $\Lambda(\pi)^*$ the subset of non-zero weights. Denote by $V_\lambda \leq V$ the *weight subspace*, corresponding to $\lambda \in \Lambda(\pi)$ and denote by m_λ the dimension of V_λ .

A representation π is called *basic* if for every pair of non-zero weights $\lambda, \mu \in \Lambda^*(\pi)$ such that $\lambda - \mu \in \Pi$ one has $\sigma_\alpha(\lambda) = \mu$ for some $\alpha \in \Phi$. Obviously, this is equivalent to saying that $W(\Phi)$ acts transitively on $\Lambda(\pi)^*$.

The irreducible representations of Chevalley groups used in the present paper form a sublist of [16, Table 2]. More specifically, all of them are *fundamental* (i.e. their highest weight is fundamental) and *basic*. We widely employ the technique of *weight diagrams* (see [16, § 2]) to help visualize the structure of these representations. In the simplest case of a *microweight* representation π (i.e. π is basic and $V_0 = 0$) the weight diagram of (V, π) is just an undirected graph whose vertices are in the one-to-one correspondence with the elements of $\Lambda(\pi)$. Two vertices λ, μ of the diagram are joined by a bond marked i if $\lambda - \mu = \alpha_i$.

An immediate application of the weight diagrams is that they allow one to quickly read off the branching of a given basic representation with respect to a subsystem subgroup. If J is a subset of Π and Δ is the subsystem of Φ spanned by J then the weight diagram of π restricted to $G(\Delta, R)$ can be obtained from the weight diagram of π by simply removing all the bonds whose label i is such that $\alpha_i \notin J$ (cf. [16, § 2.7]).

Recall that all nonzero weights of a basic representation have multiplicity one and the multiplicity m_0 of the zero weight subspace equals $|\Delta(\pi)|$, where $\Delta(\pi) = \Lambda(\pi)^* \cap \Pi$ (see [13, Lemma 2.1]). For $\alpha \in \Phi$ one can define certain elements $e_0(\alpha) \in V_0$ and $\alpha_* \in V_0^* = \text{Hom}_R(V_0, R)$ and choose some set of vectors $E^* = \{e_\lambda\}_{\lambda \in \Lambda^*(\pi)}$ in such a way that $E_\pi = E^* \cup \{e_0(\alpha)\}_{\alpha \in \Delta(\pi)}$ forms a basis of V in which the action of the elementary root unipotents $x_\alpha(\xi)$ has a particularly simple description.

Lemma 2.3 ([13, Lemma 2.3]). *Let (V, π) be a basic representation of $G(\Phi, R)$. Then the action of $x_\alpha(\xi)$ is described by the following formulae.*

$$\begin{aligned} \text{If } \lambda \in \Lambda(\pi)^*, \lambda + \alpha \notin \Lambda(\pi), \text{ then } & x_\alpha(\xi)e_\lambda = e_\lambda; \\ \text{If } \lambda, \lambda + \alpha \in \Lambda(\pi)^*, \text{ then } & x_\alpha(\xi)e_\lambda = e_\lambda \pm \xi e_{\lambda+\alpha}; \\ \text{If } \alpha \notin \Lambda(\pi)^*, \text{ then } & x_\alpha(\xi)v_0 = v_0 \text{ for any } v_0 \in V_0; \\ \text{If } \alpha \in \Lambda(\pi)^*, \text{ then } & x_\alpha(\xi)e_{-\alpha} = e_{-\alpha} \pm \xi e_0(\alpha) \pm \xi^2 e_\alpha \text{ and} \\ & x_\alpha(\xi)v_0 = v_0 \pm \xi \alpha_*(v_0)e_\alpha \text{ for } v_0 \in V_0. \end{aligned}$$

The statement of the above lemma can be visualized using the weight diagrams, see [16, § 3.4]. Although it is possible to fix the signs in the statement of the above lemma, we make no attempt to do this and refer the reader to [30].

Notice that the highest weight of the natural representations of the classical groups is ϖ_1 . It will be convenient for us to number the weights of these representations as in [18, § 1B]:

$$\begin{array}{ll} 1, 2, \dots, \ell + 1 & \text{in the case } \Phi = \mathbf{A}_\ell, \\ 1, 2, \dots, \ell, 0, -\ell, \dots, -2, -1 & \text{in the case } \Phi = \mathbf{B}_\ell, \\ 1, 2, \dots, \ell, -\ell, \dots, -2, -1 & \text{in the cases } \Phi = \mathbf{C}_\ell, \mathbf{D}_\ell. \end{array}$$

For example, we write 1 instead of ϖ_1 , 2 instead of $\varpi_1 - \alpha_1$ etc.

Let $\lambda_1, \lambda_2 \in \Lambda(\pi)$ be a pair of weights of a representation π such that $\lambda_1 - \lambda_2 \in \Phi$. It will be convenient for us to write $x_{\lambda_1, \lambda_2}(\xi)$ instead of $x_{\lambda_1 - \lambda_2}(\xi)$. For example, for $\Phi = \mathbf{A}_\ell$ we have $x_{1,2}(\xi) = x_{1-2}(\xi) = x_{\varpi_1 - \varpi_1 + \alpha_1}(\xi) = x_{\alpha_1}(\xi)$.

2.4. Relative Chevalley groups. Recall from the introduction that the elements $z_\alpha(s, \xi) = x_\alpha(s)^{x_{-\alpha}(\xi)}$ generate $E(\Phi, R, I)$ as an abstract group.

Lemma 2.4 ([19, Corollary 3.3]). *Let Φ be a root system of rank ≥ 2 , let R be a commutative ring and $I \trianglelefteq R$ be its ideal. If $\Phi \neq \mathbf{C}_\ell$ then $E(\Phi, R, I^2) \leq E(\Phi, I)$, otherwise $E(\Phi, R, II^2) \leq E(\Phi, I)$.*

Here I^2 denotes the ideal generated by the squares a^2 , where $a \in I$. Recall also that I^2 is generated by the products ab for all $a, b \in I$. Clearly, II^2 is generated by the elements of the form a^2b for $a, b \in I$.

For a special subset of roots $\Sigma \subseteq \Phi$ we denote by $U(\Sigma, I)$ the subgroup spanned by all $x_\alpha(I)$ for $\alpha \in \Sigma$. Let $J \subset \Pi$. The subgroup $U(\Sigma_J^+, I)$ is normalized by $E(\Delta_J, R)$, hence the Minkowski product set $EP_J(R, I) = E(\Delta_J, R, I) \cdot U(\Sigma_J^+, I)$ is a subgroup called a *standard parabolic subgroup*. The following two equalities will be referred to in the sequel as the *Levi decomposition*:

$$(2.7) \quad EP_J(R, I) = U(\Sigma_J^+, I) \cdot E(\Delta_J, R, I) = E(\Delta_J, R, I) \cdot U(\Sigma_J^+, I).$$

When $J = \{\alpha_s\}$ for some $1 \leq s \leq \ell$, we use the shorthand $EP_s(R, I)$ for $EP_{\{\alpha_s\}}(R, I)$. When $I = R$, we also write $EP_J(R)$ instead of $EP_J(R, R)$.

Denote by $H(\Phi, R)$ the subgroup generated by all $h_\alpha(\varepsilon)$, $\alpha \in \Phi$, $\varepsilon \in R^*$, and set

$$H(\Phi, R, I) = H(\Phi, R) \cap G(\Phi, R, I) = \langle h_\alpha(\varepsilon), \alpha \in \Phi, \varepsilon \in R^* \cap (1 + I) \rangle.$$

Consider an element $\varepsilon \in R^* \cap (1 + I)$, and rewrite it as $\varepsilon = 1 + s$, $s \in I$. The element $h_\alpha(\varepsilon)$ can be expressed as

$$(2.8) \quad \begin{aligned} h_\alpha(1 + s) &= x_\alpha(-1) x_{-\alpha}(-s) x_\alpha((1 + s)^{-1}) x_{-\alpha}(s(1 + s)) = \\ &= x_\alpha((1 + s)^{-1} - 1) z_{-\alpha}(-s, (1 + s)^{-1}) x_{-\alpha}(s(1 + s)). \end{aligned}$$

Note that $(1 + s)^{-1} \in 1 + I$ and so all the factors lie in $E(\Phi, R, I)$. This shows, in particular, that $H(\Phi, R, I) \leq E(\Phi, R, I)$.

The following lemma is a relative version of the classical result sometimes called the Chevalley—Matsumoto decomposition. It can be deduced easily from the absolute statement (see [18, Theorem 1.3]).

Lemma 2.5. *Let π be a basic fundamental representation of $G_{sc}(\Phi, R)$ with the highest weight ϖ_s . Assume that $g \in G_{sc}(\Phi, R, I)$ is such that $(g \cdot v^+)_{\varpi_s} = 1$, then*

$$g \in U(\Sigma_s^-, I) \cdot G_{sc}(\Delta_s, R, I) \cdot U(\Sigma_s^+, I).$$

2.5. K_1 -functor modeled on Chevalley groups. Recall that by a theorem of Taddei $E(\Phi, R)$ is a normal subgroup of $G_{sc}(\Phi, R)$ provided Φ is an irreducible root system of rank ≥ 2 (see [21]).

Using standard relativization argument it is not hard to deduce from Taddei's result that $E(\Phi, R, I)$ is normal in $G(\Phi, R, I)$ under the same assumptions on Φ . This allows us to define the relative K_1 -group as $K_1(\Phi, R, I) = G(\Phi, R, I)/E(\Phi, R, I)$. When $I = R$, we write $K_1(\Phi, R)$ for $K_1(\Phi, R, R)$.

In some cases it is known that $K_1(\Phi, R, I)$ is trivial. For example, $SK_1(\ell + 1, R) = K(A_\ell, R) = 1$ for any ring of stable rank 1 (see section 3), and for other root systems some stronger assumption is required such as $\text{asr}(R) = 1$ or being semilocal. For any Euclidean ring $K_1(\Phi, R, I)$ is trivial for every root system Φ .

Let k be a global field, S be a set of places of k , \mathcal{O}_S be the Dedekind ring of arithmetic type defined by S and I be an ideal of \mathcal{O}_S .

Proposition 2.6. *Let Φ be a root system of rank ≥ 2 . Assume that the field k has a real embedding. Then $K_1(\Phi, \mathcal{O}_S, I) = 1$.*

Proof. Follows from [3, Theorem 3.6] and [13, Corollary 4.5]. \square

3. STABILITY CONDITIONS

In this section we define the stability conditions used in the statements of our decomposition theorems in section 4. First, we recall the notion of the stable rank of an ideal introduced by L. Vaserstein in [27, 28]. As we will be mainly concerned with applications to Chevalley groups, our exposition of the stable ranks is necessarily limited to commutative rings. The main goal of subsection 3.2 is to define the relative version of the absolute stable rank condition, which generalizes the definition in [6, 12]. Finally, in the end of this section we state several technical lemmas describing the action of certain unipotent radicals on the unimodular columns under the assumption of a suitable stability condition.

3.1. Relative stable rank. Recall that a row $a \in {}^nR$ is called *I -unimodular* if it is congruent to $(1, 0, \dots, 0)$ modulo I and its components a_1, a_2, \dots, a_n generate R as an ideal. A column $b \in R^n$ is called *I -unimodular* if its transpose b^t is an I -unimodular row. We denote the set of all I -unimodular rows (resp. columns) by $\text{Umd}(n, I)$ (resp. $\text{Ums}(n, I)$). When $I = R$, we refer to the R -unimodular rows and columns as simply *unimodular*.

It is not hard to show that for an I -unimodular row a there exists an I -unimodular column b such that $ab = 1$ (see [27, § 2]).

An I -unimodular row $a = (a_1, \dots, a_{n+1})$ is called *stable* if one can choose $b_1, \dots, b_n \in I$ such that the row $(a_1 + a_{n+1}b_1, \dots, a_n + a_{n+1}b_n)$ is also I -unimodular. We say that I satisfies the stable range condition $\text{SR}_n(I)$ if any I -unimodular row of length $n+1$ is stable. Vaserstein noted [28, Theorem 1] that $\text{SR}_n(I)$ implies $\text{SR}_m(I)$ for any $m \geq n$. It is also clear that the condition $\text{SR}_n(I)$ does not depend on the choice of the ambient ring R . By definition, the *stable rank* of I (denoted $\text{sr}(I)$) is the smallest natural number n such that $\text{SR}_n(I)$ holds (we set $\text{sr}(I) = \infty$ if no such n exists).

The following proposition summarizes the basic properties of the stable rank.

Proposition 3.1. *Let R be an arbitrary commutative unital ring and let $I \trianglelefteq R$ be an ideal.*

- (1) *For any ideal $I' \subseteq I$ one has $\text{sr}(I') \leq \text{sr}(I)$, $\text{sr}(I/I') \leq \text{sr}(I)$;*

- (2) One has $\text{sr}\left(\prod_{i=1}^n R_i\right) = \max_{i=1}^n (\text{sr}(R_i))$;
- (3) Let $J(R)$ denote the Jacobson radical of R , then $\text{sr}(R) = \text{sr}(R/J(R))$ and $\text{sr}(J(R)) = 1$;
- (4) Let $I \rtimes \mathbb{Z}$ denote the ring obtained by formally adjoining 1 to I . Then $\text{sr}(I \rtimes \mathbb{Z}) = \max(2, \text{sr}(I))$.

Proof. See [27, Theorem 2.3], [28]. □

Example 3.2. Since the stable rank of a field equals 1, one can conclude from the previous proposition that $\text{sr}(R) = 1$ for any semilocal ring R . Other examples of rings of stable rank 1 are provided by the Boolean rings, the ring of all algebraic integers, the ring of entire functions, the disk-algebra, etc. For this and many other examples see [25].

3.2. Relativization of the absolute stable rank. For a row $a = (a_1, \dots, a_n) \in {}^nR$ denote by $\mathfrak{J}(a)$ the intersection of all maximal ideals of R containing a_1, \dots, a_n . It is easy to see that a row $a \in R^n$ is unimodular if and only if $\mathfrak{J}(a) = R$. Clearly, for any $g \in \text{GL}(n, R)$ one has $\mathfrak{J}(a \cdot g) = \mathfrak{J}(a)$.

Definition 3.3. We say that a row $a = (a_1, \dots, a_{n+1}) \in {}^{n+1}I$ can be *I-shortened*, if there exist $c_1, \dots, c_n \in I$ such that $\mathfrak{J}(a_1, \dots, a_{n+1}) = \mathfrak{J}(a_1 + c_1 a_{n+1}, \dots, a_n + c_n a_{n+1})$.

Definition 3.4. We say that an ideal I satisfies the condition $\text{ASR}_n(I)$ if it satisfies $\text{SR}_n(I)$ and, moreover, any row $a \in {}^{n+1}I$ can be *I-shortened*.

It is easy to see that $\text{ASR}_m(I)$ implies $\text{ASR}_n(I)$ for any $n \geq m$. By definition, the *absolute relative stable rank* $\text{asr}(I)$ is the smallest natural n such that $\text{ASR}_n(I)$ holds (again we set $\text{asr}(I) = \infty$ if no such n exists).

A priori our definition of $\text{ASR}_n(I)$ depends on R . Below we will see that in fact there is no such dependence. The following lemma is a relative version of [12, Lemma 8.2].

Lemma 3.5. *For a commutative ring R and an ideal $I \trianglelefteq R$ the following statements are equivalent:*

- (1) Any row $a \in {}^{n+1}I$ can be *I-shortened*;
- (2) For any *I*-unimodular row $(b, a_1, \dots, a_n, d) \in \text{Umd}(n+2, I)$ there exist $c_1, \dots, c_n \in I$ such that $(b + b', a_1 + c_1 d, \dots, a_n + c_n d)$ is *I*-unimodular for any $b' \in J$, where $J = I \cdot a_1 + \dots + I \cdot a_n + I \cdot d \leq I$.

Proof. Assume first that any row $a \in {}^{n+1}I$ can be *I-shortened*. In particular, for a given *I*-unimodular row $(b, a_1, \dots, a_n, d) \in \text{Umd}(n+2, I)$ there exist c_1, \dots, c_n such that

$$\mathfrak{J}(a_1, \dots, a_{n+1}) = \mathfrak{J}(a_1 + c_1 a_{n+1}, \dots, a_n + c_n a_{n+1}).$$

Therefore $(b, a_1 + c_1 d, \dots, a_n + c_n d)$ is also unimodular. Of course, for any $b' \in J$ we could replace b with $b + b'$ from the very start.

To show the converse take an arbitrary row $(a_1, \dots, a_n, d) \in {}^{n+1}I$ and consider the *I*-unimodular row $(1, a_1, \dots, a_n, d) \in \text{Umd}(n+2, I)$. By the hypothesis, there exist $c_1, \dots, c_n \in I$ such that

$$v = (1 + b', a'_1, \dots, a'_n) = (1 + b', a_1 + c_1 d, \dots, a_n + c_n d)$$

is unimodular for any $b' \in J$. Assume that there exists a maximal ideal $\mathfrak{m} \trianglelefteq R$ such that all a'_1, \dots, a'_n are contained in \mathfrak{m} , but at least one of the elements d, a_i is not. Then clearly

$d \notin \mathfrak{m}$ and $I \not\subseteq \mathfrak{m}$ (otherwise $a_i = a'_i - c_i d \in \mathfrak{m}$, contrary to the assumption). Now we can find $t \in I$ such that its image \bar{t} in the residue field R/\mathfrak{m} equals $-\bar{1}/\bar{d}$. This means that $1 + b' \in \mathfrak{m}$ for $b' = td \in J$ which, contradicts the unimodularity of v . This shows that no such \mathfrak{m} may exist and, therefore, $\mathfrak{J}(a'_1, \dots, a'_n) = \mathfrak{J}(a_1, \dots, a_n, d)$. \square

Obviously, the second statement of Lemma 3.5 does not depend on R , hence, as suggested by the notation, $\text{asr}(I)$ is independent of R .

Let R be a commutative ring. We denote by $\text{Max}(R)$ its *maximum spectrum*, i.e. the set of maximal ideals of R , equipped with the Zariski topology. For a topological space X denote by $\dim(X)$ its usual topological dimension. From the definition of $\text{asr}(I)$ and [6, Theorem 2.3] (or [12, Theorem 3.7]) it follows that

$$(3.1) \quad \text{sr}(I) \leq \text{asr}(I) \leq \text{asr}(R) \leq \dim(\text{Max}(R)) + 1 \leq \dim(\text{Spec}(R)) + 1.$$

There exist examples of rings for which the first inequality in the above formula is strict. More precisely, there are rings of stable rank 1 but of absolute stable rank ≥ 2 , see [12]. On the other hand, [12, Theorem 1.3] shows that $\text{sr}(R) = \text{asr}(R)$ for any principal ideal ring R .

Example 3.6. From inequality (3.1) one concludes, in particular, that

- $\text{asr}(R) = 1$ for every semilocal ring R ;
- $\text{asr}(R) \leq 2$ for every Dedekind domain R ;
- $\text{asr}(A[x]) \leq 3$ for every locally principal ring A ;
- $\text{asr}(F[x_1, \dots, x_n]) \leq n + 1$ for any field F .

For certain classes of fields there is also a lower estimate for $\text{sr}(F[x_1, \dots, x_n])$ which allows to compute precisely the value of both $\text{sr}(R)$ and $\text{asr}(R)$. For example, $\text{sr}(F[x, y]) = 3$ for every F with $K_2^M(F) \neq 0$ (see [9]) and $\text{sr}(F[x_1, \dots, x_n]) = n + 1$ for $F \subseteq \mathbb{R}$, see [28, Theorem 8]. Notice also that $\text{sr}(\mathbb{Z}[x]) = 3$ (see [7]) and $\text{sr}(\mathbb{Z}[x_1, \dots, x_n]) = n + 1$ for $n > 1$ (see example after [29, Theorem 18.2]).

3.3. Action of unipotent radicals.

Lemma 3.7. *Let $v = (v_1, \dots, v_n)^t$ be a column. Denote by v' the vector composed of squares of the components of v , i. e. $v' = (v_1^2, \dots, v_n^2)^t$. Then for any matrix $b \in M(n, I)$ one can find a symmetric matrix $a \in M(n, I)$, $a = a^t$ such that $b \cdot v' = a \cdot v$.*

Proof. Straightforward computation shows that the assertion of lemma holds for the matrix a defined by

$$a_{ij} = b_{ij}v_j + b_{ji}v_i, \quad j \neq i, \quad a_{ii} = b_{ii}v_i - \sum_{\substack{j=1 \\ j \neq i}}^{\ell} b_{ji}v_j. \quad \square$$

Let $v \in V = R^{2\ell}$ be a vector of the natural representation of $G(D_\ell, R)$. Denote by v_+ and v_- the upper and the lower halves of v , i. e. $v_+ = (v_1, \dots, v_\ell)^t$, $v_- = (v_{-\ell}, \dots, v_{-1})^t$.

Lemma 3.8. *For any I -unimodular column $v = (v_+, v_-)^t \in \text{Ums}(2\ell, I)$ there exists $g \in \text{U}(\Sigma_\ell^+, I) \leq \text{E}(\Phi, R, I)$ such that $(g \cdot v)_+ \in \text{Ums}(\ell, I)$ under the following assumptions on Φ and I .*

- (1) $\Phi = C_\ell$ and $\text{sr}(I) \leq \ell$;
- (2) $\Phi = D_\ell$ and $\text{asr}(I) \leq \ell - 1$.

Proof. CASE $\Phi = C_\ell$. Denote by p the matrix of size ℓ such that its only nonzero entries equal 1 and are on the skew-diagonal, i.e. $p_{ij} = \delta_{i, \ell-j+1}$. For $b \in M(\ell, I)$ set $g(b) = \begin{pmatrix} e_\ell & p \cdot b \\ 0 & e_\ell \end{pmatrix}$. Clearly, if b is symmetric then $g(b)$ lies in $U(\Sigma_\ell^+, I) \leq E(C_\ell, R, I)$.

Notice that the column $v' = (v_1, \dots, v_\ell, v_{-\ell}^2, \dots, v_{-1}^2)^t$ is I -unimodular. By the definition of the relative stable rank we can find a matrix $b \in M(\ell, I)$ such that the upper half v'_+ of the vector $v'' = g(b) \cdot v'$ is I -unimodular. It is clear that $v''_+ = v_+ + pbv'_-$. Finally, applying Lemma 3.7, we find a symmetric matrix a such that

$$(g(a) \cdot v)_+ = v_+ + pav_- = v_+ + pbv'_- = v''_+ \in \text{Ums}(\ell, I).$$

CASE $\Phi = D_\ell$. Denote by J the ideal of R spanned by the components of v_- . Clearly, $J \subseteq I$. By Proposition 3.1 $\text{sr}(I/J) \leq \ell - 1$, therefore the elementary group $E(A_{\ell-1}, R/J, I/J)$ acts transitively on $\text{Ums}(\ell, I/J)$ (see [27, Theorem 2.3c]). This implies the existence of an element $h \in E(\Delta_\ell, R, I)$ such that the vector $v' = h \cdot v$ satisfies $v'_i \equiv \delta_{i1} \pmod{J}$ for $i = 1, \dots, \ell$.

Clearly, $(v'_1, v'_{-\ell}, \dots, v'_{-1})$ is I -unimodular. Applying Lemma 3.5(ii), we find $c_2, \dots, c_\ell \in I$ such that for $v'' = \prod_{i=2}^\ell x_{-i,-1}(c_i) \cdot v'$ one has $(v''_1, v''_{-\ell}, \dots, v''_{-2}) \in \text{Ums}(\ell + 1, I)$. Now, applying the condition $\text{sr}(I) \leq \ell - 1$ once again, we find $d_1, d_3, \dots, d_\ell \in I$ such that the entries $(v'''_1, v'''_{-\ell}, \dots, v'''_{-3})$ of $v''' = x_{-2,1}(d_1) \cdot \prod_{i=3}^\ell x_{-2,-i}(d_i) \cdot v''$ form an I -unimodular column.

We can find $f_1, f_3, \dots, f_\ell \in R$ such that $f_1 v'''_1 + \sum_{i=3}^\ell f_i v'''_{-i} = 1$. Set $\xi = v'''_1 - v'''_{-2} - 1 \in I$, $v^{(4)} = x_{1,2}(\xi f_1) \cdot \prod_{i=3}^\ell x_{-i,2}(\xi f_i) \cdot v'''$. Clearly $v^{(4)}_2 = v^{(4)}_1 - 1$, therefore $v^{(4)}_+$ is I -unimodular. Summarizing the above, we have found $g \in \text{EP}_\ell(R, I)$ such that $v^{(4)} = g \cdot v$ and the assertion of the lemma immediately follows from the Levi decomposition. \square

Corollary 3.9. *Denote by i the standard embedding $G(B_{\ell-1}, R, I) \hookrightarrow G(D_\ell, R, I)$. If $\text{asr}(I) \leq \ell - 1$, then for every I -unimodular column $v \in \text{Ums}(2\ell, I)$ there exists $g \in U(\Sigma_{\ell-1}^+, I) \leq E(B_{\ell-1}, R, I)$ such that the upper half of the vector $i(g) \cdot v$ forms an I -unimodular column of height ℓ .*

Proof. The assertion follows from the fact that for every $u \in U(\Sigma_\ell^+, I) \leq E(D_\ell, R, I)$ one can find $u' \in G(\Delta_\ell, R, I)$ such that uu' lies in the image of i . Indeed, denote by σ the symmetry of the Dynkin diagram of D_ℓ , and decompose u into the product $u_1 \cdot u_2$, where $u_1 \in U(\Sigma_\ell^+ \cap \Delta_{\ell-1}, I)$ and $u_2 \in U(\Sigma_\ell^+ \cap \Sigma_{\ell-1}^+, I)$. Then one takes $u' = \sigma(u_1)$.

Now by Lemma 3.8(ii) one finds a suitable $u \in U(\Sigma_\ell^+, I) \leq E(D_\ell, R, I)$ which makes the upper half unimodular, and since u' lies in $G(\Delta_\ell, R, I)$, the upper half remains unimodular. \square

Lemma 3.10. *Let $\Phi = A_\ell, C_\ell, D_\ell$. Denote by π the natural representation of $G(\Phi, R)$ on $V = R^n$, $n = \ell + 1, 2\ell, 2\ell$ respectively. Assume that one of the following assumptions holds:*

- (1) $\Phi = A_\ell$, $\Gamma = \{k + 1, \dots, \ell + 1\} \subset \Lambda(\pi)$ and $\text{sr}(I) \leq k \leq \ell$;
- (2) $\Phi = C_\ell$, $\Gamma = \{-\ell, \dots, -2, -1\} \subset \Lambda(\pi)$ and $\text{sr}(I) \leq \ell$;
- (3) $\Phi = D_\ell$, $\Gamma = \{-\ell, \dots, -2, -1\} \subset \Lambda(\pi)$ and $\text{asr}(I) \leq \ell - 1$.

Then for any $g \in G(\Phi, R, I)$ there exist $x \in U(\Phi^+, I)$, $y \in U(\Phi^-, I)$ such that $(y x g \cdot v^+)_\lambda = 0$ for all $\lambda \in \Gamma$.

Proof. Denote by v the image of the highest weight vector v^+ under g .

CASE $\Phi = A_\ell$. From the definition of the relative stable rank it follows that we can find $x = \begin{pmatrix} e_k & a \\ 0 & e_{n-k} \end{pmatrix} \in U(\Sigma_k^+, I)$ such that the upper k components of $v' = x \cdot v$ form an

I -unimodular column. Now, to obtain zeroes at the desired positions it remains to subtract from $v'_{k+1}, \dots, v'_{\ell+1}$ suitable multiples of v'_1, \dots, v'_k . This operation corresponds to the left multiplication by some element $y \in U(\Sigma_k^-, I)$.

CASE $\Phi = C_\ell$. Applying Lemma 3.8.(i), we find $x \in U(\Sigma_\ell^+, I)$ such that the upper half v'_+ of $v' = x \cdot v$ is unimodular. Set $g(a) = \begin{pmatrix} e_\ell & 0 \\ p \cdot a & e_\ell \end{pmatrix}$. Clearly, if a is symmetric, then $g(a) \in U(\Sigma_\ell^-, I)$. Since the column $v''_+ = (v_1'^2, \dots, v_\ell'^2)^t$ is I -unimodular, there exists a matrix $b \in M(\ell, I)$ such that $v'_- + pbv''_+ = 0$. Finally, using Lemma 3.7, we find a symmetric matrix a such that $(g(a) \cdot v')_- = pav'_+ + v'_- = pbv''_+ + v'_- = 0$.

CASE $\Phi = D_\ell$. From the proof of Lemma 3.8.(ii) it follows that there exists $h_1 \in \text{EP}_\ell(R, I)$ such that for $v' = h_1 \cdot v$ one has $v'_2 = v'_1 - 1 \in I$. Clearly, for $v'' = z_{-\alpha_2}(-v'_2, 1) \cdot v'$ one has $v''_1 = 1$, hence by Lemma 2.5 there exists $h_2 \in U(\Phi^-, I)$ such that the element $g' = h_2 \cdot z_{-\alpha_2}(-v'_2, 1) \cdot h_1 \cdot g$ fixes v^+ . Using the Levi decomposition we can write $g' = h \cdot y \cdot x \cdot g$ for some $y \in U(\Sigma_\ell^-, I)$, $x \in U(\Sigma_\ell^+, I)$, $h \in E(\Delta_\ell, R, I)$. It is clear that x, y are the desired elements. \square

4. RELATIVE PARABOLIC FACTORIZATIONS

In this section we formulate and prove the relative versions of the decompositions from [18], which will be the main technical tools throughout the next section.

4.1. Relative Gauss decomposition. The proof of the Gauss decomposition presented below is similar to the absolute case (cf. [17, Theorem 5.1]).

Proposition 4.1. *Let Φ be a reduced irreducible root system of rank ℓ and let Δ_1, Δ_ℓ be two reductive subsystems of Φ , corresponding to the endnodes of the Dynkin diagram of Φ . Suppose that both relative elementary subgroups $E(\Delta_i, R, I)$, $i = 1, \ell$ admit the triangular decomposition with N triangular factors:*

$$E(\Delta_i, R, I) = H(\Delta_i, R, I) \cdot U(\Delta_i^+, I) \cdot U(\Delta_i^-, I) \cdot \dots \cdot U(\Delta_i^\pm, I), \quad i = 1, \ell.$$

Then the ambient group $E(\Phi, R, I)$ admits the decomposition with the same number of factors:

$$E(\Phi, R, I) = H(\Phi, R, I) \cdot U(\Phi^+, I) \cdot U(\Phi^-, I) \cdot \dots \cdot U(\Phi^\pm, I).$$

Proof. Denote by Y the product of subgroups in the right-hand side of the above equality. To show that $Y = E(\Phi, R, I)$ it suffices to check that

- (1) Y is normalized by $E(\Phi, R)$, i. e. $Y^{E(\Phi, R)} \subseteq Y$;
- (2) there exists a set X , generating $E(\Phi, R, I)$ as a *normal* subgroup of $E(\Phi, R)$ such that $XY \subseteq Y$.

To prove the first assertion it suffices to show that $Y^{x_\alpha(\xi)} \subseteq Y$ for any $\alpha \in \pm\Pi$, $\xi \in R$. Fix a root $\alpha \in \pm\Pi$. Clearly, $\alpha \in \Delta_i$ for $i = 1$ or for $i = \ell$, and we can expand Y as follows:

$$Y = H(\Phi, R, I) \cdot U(\Delta_i^+, I) \cdot \dots \cdot U^\pm(\Delta_i, I) \cdot U(\Sigma_i^+, I) \cdot \dots \cdot U(\Sigma_i^\pm, I).$$

For every $h \in H(\Phi, R, I)$ one has for some $s \in I$

$$x_\alpha(\xi) \cdot h = h \cdot x_\alpha((1+s)\xi) = h \cdot x_\alpha(\xi) x_\alpha(s\xi).$$

Therefore by the assumption of the theorem

$$\begin{aligned} Y^{x_\alpha(\xi)} &\subseteq H(\Phi, R, I) \cdot x_\alpha(-\xi) \cdot X_\alpha(I) \cdot E(\Delta_i, R, I) \cdot x_\alpha(\xi) \cdot U(\Sigma_i^+, I) \cdot \dots \cdot U(\Sigma_i^\pm, I) = \\ &= H(\Phi, R, I) \cdot E(\Delta_i, R, I) \cdot U(\Sigma_i^+, I) \cdot \dots \cdot U(\Sigma_i^\pm, I) = Y. \end{aligned}$$

Now set $X = \{x_\alpha(\xi) \mid \alpha \in \Pi, \xi \in I\}$. Every root is a conjugate of some fundamental root under the action of $W(\Phi)$. Since $E(\Phi, R)$ contains the normalizer of the torus, the set $X^{E(\Phi, R)}$ contains all the generators of the group $E(\Phi, I) = \langle x_\alpha(\xi), \alpha \in \Phi, \xi \in I \rangle$. Finally, the inclusion $XY \subseteq Y$ follows from the fact that $H(\Phi, R, I)$ normalizes every root subgroup $X_\alpha(I)$. \square

Proof of Theorem 1. In view of the above proposition it suffices to prove that the Gauss decomposition of length 3 holds for $\Phi = A_1$.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $SL(2, R, I)$. The first column of A is I -unimodular, therefore there exists $z \in I$ such that $a + cz \in R^*$. Multiplying A on the left by $x_{12}(z)$, we get a matrix $A' = x_{12}(z) \cdot A = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ with the invertible element a' in the top-left corner. After multiplying A' on the left by $x_{21}(-c/a')$ and on the right by $x_{12}(-b'/a')$ we get a diagonal matrix. Thus we have obtained the relative Gauss decomposition of A

$$A = x_{12}(-z) \cdot x_{21}(c/a') \cdot \begin{pmatrix} \varepsilon & 0 \\ 0 & 1/\varepsilon \end{pmatrix} \cdot x_{12}(b'/a') = x_{12}(-z) \cdot \begin{pmatrix} \varepsilon & 0 \\ 0 & 1/\varepsilon \end{pmatrix} \cdot x_{21}(y) \cdot x_{12}(b'/a'),$$

where $\varepsilon \in 1 + I$ and $y \in I$. \square

4.2. Relative Bass—Kolster decompositions. The next theorem is a relative version of the so-called Bass—Kolster decomposition (cf. [18, Theorem 2.1]).

Theorem 6. *Let Φ be a classical root system of rank $\ell \geq 2$, let R be an arbitrary commutative ring and I be an ideal, satisfying one of the following assumptions:*

$$\begin{aligned} \Phi = A_\ell, \ell \geq 2, & \quad \text{sr}(I) \leq \ell; \\ \Phi = C_\ell, \ell \geq 2, & \quad \text{sr}(I) \leq 2\ell - 1; \\ \Phi = B_\ell, D_\ell, \ell \geq 3, & \quad \text{asr}(I) \leq \ell - 1. \end{aligned}$$

Then the principal congruence subgroup $G(\Phi, R, I)$ admits the following relative version of the Bass—Kolster decomposition:

$$G(\Phi, R, I) = U(\Phi^+, I) \cdot U(\Phi^-, I) \cdot Z \cdot U(\Sigma_1^- \setminus \{-\alpha_{\max}\}, I) \cdot U(\Sigma_1, I) \cdot G(\Delta_1, R, I),$$

where $Z = Z_{\alpha_{\max}}(I) = \{z_{-\alpha_{\max}}(r, 1) \mid r \in I\}$.

Proof. Let g be an element of $G(\Phi, R, I)$. Set $v = g \cdot v^+ \in \text{Ums}(n, I)$. Notice that in each case it suffices to find $g' \in U(\Phi^-, I) \cdot U(\Phi^+, I) \cdot g$ such that

$$(4.1) \quad (g' \cdot v^+)_1 = 1 + s \text{ and } (g' \cdot v^+)_{\varpi_1 - \alpha_{\max}} = s \text{ for some } s \in I.$$

Indeed, set $g'' = z_{-\alpha_{\max}}(-s, 1) \cdot g'$. Obviously, one has $(g'' \cdot v^+)_1 = 1$, $(g'' \cdot v^+)_{\varpi_1 - \alpha_{\max}} = 0$ and the conclusion of the theorem follows from Lemma 2.5.

CASE $\Phi = A_\ell$, $n = \ell + 1$. Since $\text{sr}(I) \leq \ell$, one can find $a_1, \dots, a_\ell \in I$ such that $(v_1 + a_1 v_{\ell+1}, \dots, v_\ell + a_\ell v_{\ell+1})^t = (v'_1, \dots, v'_\ell)^t$ is I -unimodular. Then there are $b_1, \dots, b_\ell \in I$ such that $b_1 v'_1 + \dots + b_\ell v'_\ell = v' - 1 \in I$. Thus the vector

$$v'' = \prod_{i=1}^{\ell} x_{\ell+1, i}(b_i) \cdot \prod_{i=1}^{\ell} x_{i, \ell+1}(a_i) \cdot v$$

satisfies the equalities (4.1).

CASE $\Phi = C_\ell$, $n = 2\ell$. Notice that the column $(v_1, \dots, v_{-2}, v_{-1}^2)^t$ is also I -unimodular. Applying the assumption $\text{sr}(I) \leq 2\ell - 1$, we find $c_1, c_2, \dots, c_{-2} \in I \cdot v_{-1}$ such that upper

$2\ell - 1$ components of $v' = (v_1 + c_1 v_{-1}, \dots, v_{-2} + c_{-2} v_{-1}, v_{-1})^t$ form an I -unimodular column. By the choice of c_i we can find suitable $d \in I$ such that $h_1 \cdot v = v'$ for

$$h_1 = x_{1,-1}(c_1 + d) \cdot \prod_{i=2}^{-2} x_{i,-1}(c_i) \in U(\Sigma_1^+, I).$$

We can find $f_1, f_2, \dots, f_{-2} \in R$ such that $f_1 v'_1 + \sum_{i=2}^{-2} f_i v'_i = 1$. Set $\xi = v''_1 - v''_{-1} - 1 \in I$,

$$h_2 = x_{-1,1} \left(\xi f_1 + \sum_{i=2}^{\ell} v'_1 \xi^2 f_i f_{-i} \right) \cdot \prod_{i=2}^{-2} x_{-1,i}(\xi f_i) \in U(\Sigma_1^-, I).$$

Direct computation shows that the vector $v'' = h_2 \cdot v'$ satisfies equalities (4.1).

CASE $\Phi = D_\ell$, $n = 2\ell$. By Lemma 3.8.(ii) we can find $h_1 \in U(\Sigma_\ell^+, I)$ such that the upper half v'_+ of $v' = h_1 \cdot v$ is I -unimodular. Since $\text{sr}(I) \leq \ell - 1$, we can find $c_1, c_3, \dots, c_\ell \in I$ such that $(v''_1, v''_3, \dots, v''_\ell) \in \text{Ums}(\ell - 1, I)$, where

$$v'' = h_2 \cdot x_{1,2}(c_1) \cdot v', \quad h_2 = \prod_{i=3}^{\ell} x_{i,2}(c_i).$$

We can find $f_1, f_3, \dots, f_\ell \in R$ such that $f_1 v''_1 + \sum_{i=3}^{\ell} f_i v''_i = 1$. As before, set

$$\xi = v''_1 - v''_{-2} - 1 \in I, \quad h_3 = x_{-2,1}(\xi f_1) \cdot \prod_{i=3}^{\ell} x_{-2,i}(\xi f_i), \quad v''' = h_3 \cdot v''.$$

Clearly, $t_{1,2}(c_1) \cdot h_1 \in U(\Phi^+, I)$, $h_3 \cdot h_2 \in U(\Phi^-, I)$ and v''' satisfies (4.1).

CASE $\Phi = B_\ell$, $n = 2\ell + 1$. Subdivide $v \in \text{Ums}(2\ell + 1, I)$ as $v = (v_+, v_0, v_-) \in R^\ell \times R \times R^\ell$. Denote by $J \leq I$ the ideal spanned by the components of v_- . Since $\text{sr}(I/J) \leq \ell$, we can find $c_1, \dots, c_\ell \in I$ such that for $v' = h \cdot v$, $h = \prod_{i=1}^{\ell} x_{i,0}(c_i) \in U(\Phi^+, I)$ one has $\bar{v}'_+ = (v'_1, \dots, v'_\ell) \in \text{Ums}(\ell, I/J)$ and, therefore, $(v'_+, v'_-) \in \text{Ums}(2\ell, I)$. Now the proof can be finished by repeating the argument for the case $\Phi = D_\ell$ (applied to the subset of long roots of B_ℓ). \square

It is easy to see that the proof of the above theorem is effective and gives an estimate of the total number of elementary root unipotents involved in the decomposition.

Corollary 4.2. *In the assumptions and notation of Theorem 6 every element of $G(\Phi, R, I)$ can be factored into a product of one element of $G(\Delta_1, R, I)$, one element of Z and at most $4|\Sigma_1| - 1$ elements of \mathcal{X} .*

Proof. The assertion can be obtained by a careful analysis of the proof of the previous theorem. Cases $\Phi = A_\ell, C_\ell$ are immediate. In the case $\Phi = D_\ell$ from the proof of Theorem 6 one obtains that

$$G(\Phi, R, I) = U(\Sigma_\ell^+, I) \cdot X_{\alpha_1}(I) \cdot U(\Sigma_2^- \cap \Delta_1, I) \cdot X_{-\alpha_{\max}}(I) \cdot Z \cdot U(\Sigma_1^-, I) \cdot U(\Sigma_1^+, I) \cdot G(\Delta_1, R, I).$$

We can present an element g of $U(\Sigma_\ell^+, I)$ as a product of $g_1 \in U(\Sigma_{1,2}^+ \cap \Sigma_\ell^+)$ and $g_2 \in U(\Delta_{1,2} \cap \Sigma_\ell^+)$. An examination of the extended Dynkin diagram of D_ℓ shows that g_2 either centralizes or normalizes all factors of the above decomposition (except the last one) and therefore can be moved to the right until it is consumed by $G(\Delta_1, R, I)$. On the other hand, g_1 is a product of at most $2\ell - 3$ elementary unipotents, while the width of $U(\Sigma_1^\pm, I)$ and

$U(\Sigma_2^- \cap \Delta_1)$ with respect to the elementary unipotents does not exceed $2\ell - 2$ and $2\ell - 4$, respectively. Summing up these upper bounds, we obtain

$$(2\ell - 3) + 1 + (2\ell - 4) + 1 + 2 \cdot (2\ell - 2) = 8\ell - 9 = 4|\Sigma_1| - 1.$$

The estimate in the case $\Phi = B_\ell$ can be obtained in a similar way. \square

Corollary 4.3. *Assume that Φ and I satisfy one of the following assumptions*

$$\begin{aligned} \Phi = A_\ell, \quad & \text{sr}(I) \leq 2, \quad N' = 3|\Phi^+| + 2\ell - 5; \\ \Phi = C_\ell, \quad & \text{sr}(I) \leq 3, \quad N' = 3|\Phi^+| + 3\ell - 6; \\ \Phi = B_\ell, D_\ell, \quad & \text{asr}(I) \leq 2, \quad N' = 4|\Phi^+| - 4. \end{aligned}$$

Then every element of $G(\Phi, R, I)$ can be decomposed into a product of one element of $G(\langle \pm \alpha_\ell \rangle, R, I) \cong \text{SL}(2, R, I)$ and at most N' elements of $\mathcal{Z}(\Sigma_\ell)$:

Proof. The assertion can be obtained by iteratively applying (for a total of $\ell - 1$ times) the decomposition of Theorem 6. The improved estimate for $\Phi = A_\ell$ (resp. C_ℓ) follows from the fact that it suffices to make only two (resp. three) additions to shorten the unimodular column in the first step of the proof of Theorem 6. \square

Proof of Theorem 4. As in the proof of the above corollary one has to iteratively apply Theorem 6. To reduce the number of SL_2 -factors involved in the decomposition one has to group into a single SL_2 -factor a pair of opposite root subgroups $X_\alpha(I)$, $X_{-\alpha}(I)$ (or $Z_{\pm\alpha}(I)$) appearing on each of the 3 junctions between the positive and negative unipotent subgroups in the Bass—Kolster decomposition. Since a total of $\ell - 1$ reductions are used, we get the estimate $N \leq N' - 3(\ell - 1) + 1$ and the assertion of Theorem 4 follows. \square

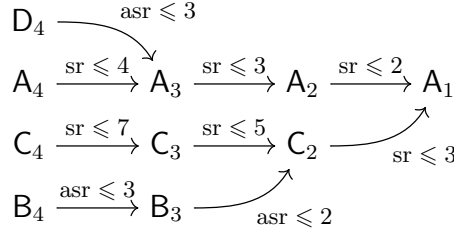


FIGURE 1. Reductions used in the proof of Corollary 4.3 and Theorem 4

4.3. Relative Dennis—Vaserstein decompositions. Let Φ be an irreducible root system of rank ℓ . In what follows, r and s are two distinct integers such that $1 \leq r, s \leq \ell$. From the Levi decomposition (2.7) it follows that the following four subsets of $E(\Phi, R, I)$ are equal:

$$\begin{aligned} A_{rs} &:= U(\Phi^+, I) \cdot U(\Phi^-, I) \cdot E(\Delta_r, R, I) \cdot \text{EP}_s(R, I) = \\ &= U(\Sigma_r^+, I) \cdot U(\Sigma_r^-, I) \cdot E(\Delta_r, R, I) \cdot \text{EP}_s(R, I) = \\ &= \text{EP}_r(R, I) \cdot E(\Delta_s, R, I) \cdot U(\Sigma_s^-, I) \cdot U(\Sigma_s^+, I) = \\ &= \text{EP}_r(R, I) \cdot U(\Sigma_r^- \cap \Sigma_s^-, I) \cdot \text{EP}_s(R, I). \end{aligned}$$

Denote by N_{rs} the submonoid of $E(\Phi, R)$, consisting of the elements which normalize the subset A_{rs} , i. e.

$$N_{rs} = \{g \in E(\Phi, R) \mid g \cdot A_{rs} \cdot g^{-1} \subseteq A_{rs}\}.$$

Lemma 4.4. *For every $\alpha \in \Delta_{r,s} \cup (\Phi^+ \setminus (\Sigma_r^+ \cap \Sigma_s^+))$ one has $X_\alpha(R) \subseteq N_{rs}$.*

Proof. Notice that for every i the group $EP_i(R, I)$ is normalized by $EP_i(R)$, hence a fortiori it is normalized by $X_\alpha(R)$, $\alpha \in S_i^+$. Since $U(\Sigma_r^- \cap \Sigma_s^-, I)$ is normalized by $E(\Delta_{\{r,s\}}, R)$, we obtain the assertion of the lemma for $\alpha \in \Delta_{r,s}$.

Now if α lies in $\Phi^+ \setminus (\Sigma_r^+ \cap \Sigma_s^+)$, then it is contained either in Δ_r or in Δ_s . Assume, for example, the latter. By the Levi decomposition we have $U(\Sigma_r^- \cap \Sigma_s^-, I)^{X_\alpha(R)} \subseteq U(\Sigma_s^-, I) \subseteq A_{rs}$, which again implies the assertion of the lemma. \square

Proof of Theorem 2. Since the equality $A_{rs} = E(\Phi, R, I)$ implies $A_{sr} = E(\Phi, R, I)$, it suffices to consider only the following possibilities for Φ , s , r :

Φ	s	r	$ \Lambda(\pi) $	type of π	type of Δ_r	$ \Lambda(\pi') $	$ \Gamma $
A_ℓ , $\ell \geq 2$	1	ℓ	$\ell + 1$	natural	$A_{\ell-1}$	ℓ	1
B_ℓ , $\ell \geq 2$	1	ℓ	$2\ell + 1$	natural	$A_{\ell-1}$	ℓ	1
C_ℓ , $\ell \geq 2$	1	ℓ	2ℓ	natural	$A_{\ell-1}$	ℓ	1
D_ℓ , $\ell \geq 4$	1	ℓ	2ℓ	natural	$A_{\ell-1}$	ℓ	2
D_ℓ , $\ell \geq 4$	ℓ	$\ell - 1$	$2^{\ell-1}$	half-spinor	$A_{\ell-1}$	ℓ	$\ell - 2$
E_ℓ , $\ell = 6, 7$	ℓ	2	27, 56	minimal	$A_{\ell-1}$	ℓ	3
E_ℓ , $\ell = 6, 7$	ℓ	1	27, 56	minimal	$D_{\ell-1}$	$2(\ell - 1)$	$\ell - 1$
F_4	4	1	26	minimal	C_3	6	3

TABLE 1. List of the cases considered in the proof of Theorem 2.

Denote by L_{rs} the set consisting of all the elements $g \in E(\Phi, R, I)$ such that $g \cdot A_{rs} \subseteq A_{rs}$. It is easy to see that L_{rs} contains $EP_r(R, I)$ and is normalized by N_{rs} , i. e. $L_{rs}^{N_{rs}} \subseteq L_{rs}$. Indeed, for $g \in N_{rs}$, $h \in L_{rs}$ one has

$$(4.2) \quad h^g \cdot A_{rs} = g^{-1} \cdot h \cdot g \cdot A_{rs} \subseteq g^{-1} \cdot h \cdot A_{rs} \cdot g \subseteq A_{rs}^g \subseteq A_{rs}.$$

The first step of the proof is to show that N_{rs} contains sufficiently many elements. This is accomplished in Lemma 4.6 below, where we invoke the stability conditions for the first time. We show that N_{rs} contains the root subgroup $X_{-\alpha_r}(R)$, which together with Lemma 4.4 and Lemma 2.2.(ii) immediately implies that N_{rs} contains the Levi subgroup $E(\Delta_s, R)$ and hence the extended Weyl group $\widetilde{W}(\Delta_s)$.

The next goal is to demonstrate the inclusion $U(\Sigma_s^+, R) \subseteq N_{rs}$ (which implies $EP_s(R) \subseteq N_{rs}$). All the possibilities for Φ , s and r fall into one of the following three cases:

- (1) *Case $m_s(\alpha_{\max}) = 1$ and Φ is simply laced.* In this case all the roots of Σ_s^+ have the same s -shape and length, hence the assertion follows from Lemma 2.2.(iii), (4.2) and the fact that we already have the inclusion $X_{\alpha_s}(R) \subseteq N_{rs}$.
- (2) *Case $\Phi = B_\ell$.* Using the argument from the previous case, we get that N_{rs} contains the subgroup generated by the root subgroups $X_\alpha(R)$, where α varies over long roots

of Σ_s^+ . It remains to prove the inclusion $X_{1,0}(R) \subset N_{rs}$. Specializing identity (2.2), we get

$$x_{1,0}(ab) = [x_{1,2}(a), x_{2,0}(b)] \cdot x_{1,-2}(-ab^2)$$

Since $X_{2,0}(R)$ and $X_{1,-2}(R)$ are contained in N_{rs} , the inclusion $X_{1,0}(R) \subseteq N_{rs}$ follows.

- (3) *Case $\Phi = \mathbf{C}_\ell, \mathbf{F}_4$.* We settle these remaining cases in Lemma 4.7, where we invoke the stability conditions one more time. In fact, we prove a stronger result, namely that N_{rs} contains $X_{-\alpha_s}(R)$ and, consequently, $N_{rs} = E(\Phi, R)$.

In view of Proposition 1.1 to prove the theorem it suffices to show that L_{rs} contains the generating set $\mathcal{Z}(\Sigma_s^-)$ of $E(\Phi, R, I)$. From the inclusion $\mathcal{Z}(\Sigma_s^-) \subseteq \mathcal{X}^{\text{EP}_s(R)}$ and (4.2) it follows that we only have to show that $\mathcal{X} \subseteq L_{rs}$.

The last inclusion follows from the same transitivity argument as above and the fact that $X_\alpha(I) \subseteq \text{EP}_r(R, I) \subseteq L_{rs}$ for $\alpha \in \Delta_r \cup \Sigma_r$. For $\Phi = \mathbf{B}_\ell$ one has to once again apply the Chevalley commutator formula (2.2):

$$X_{0,1}(I) \subseteq X_{2,1}(I) \cdot X_{2,1}(I)^{x_{0,2}(1)} \cdot X_{-2,1}(I) \subseteq L_{rs} \cdot L_{rs}^{N_{rs}} \cdot L_{rs} \subseteq L_{rs}. \quad \square$$

Lemma 4.5. *For any $1 \leq i \leq n$ the following statements hold.*

- (1) $U(\Phi^+, I) = X_{\alpha_i}(I) \cdot U(\Phi^+ \setminus \{\alpha_i\}, I) = U(\Phi^+ \setminus \{\alpha_i\}, I) \cdot X_{\alpha_i}(I)$;
- (2) *For any $\xi \in R$ one has $U(\Phi^+ \setminus \{\alpha_i\}, I)^{x_{-\alpha_i}(\xi)} \subseteq U(\Phi^+, I)$;*
- (3) $U(\Phi^+, I) \cdot U(\Phi^-, I) \subseteq U(\Phi^+ \setminus \{\alpha_i\}, I) \cdot U(\Phi^-, I) \cdot X_{\alpha_i}(I) \cdot X_{-\alpha_i}(I)$.

Proof. The first two statements easily follow from the Chevalley commutator formula (2.2) while the third one is a formal consequence of the first two. \square

Lemma 4.6. *Under the assumptions of Theorem 2 one has $X_{-\alpha_r}(R) \subseteq N_{rs}$.*

Proof. Let π be the irreducible representation of $G(\Phi, R)$ with the highest weight ϖ_s (see Table 1). Notice that Δ_r is an irreducible classical root system of type $\mathbf{A}_\ell, \mathbf{C}_\ell$ or \mathbf{D}_ℓ . Denote by (π', V') the irreducible component of the restriction of π to $G(\Delta_r, R)$ that contains the highest weight vector v^+ of π . In all the cases under consideration, π' is isomorphic to the natural representation of $G(\Delta, R)$. Set $\Gamma = \{\lambda \in \Lambda(\pi') \mid \lambda - \alpha_r \in \Lambda(\pi)\}$.

The set Γ can be visualized using the weight diagrams in the following manner. After the removal of all bonds marked r the weight diagram of π splits into several connected components. The subset $\Lambda(\pi') \subseteq \Lambda(\pi)$ corresponds to the component of the diagram that contains the vertex marked ϖ_s . Clearly, Γ consists of the weights of $\Lambda(\pi')$ incident to the removed bonds.

By a consideration of the weight diagrams (see [16]) we determine the number of elements in $\Lambda(\pi')$ and Γ (see Table 1).

Consider the subset $B \subset E(\Delta_r, R, I)$, consisting of all elements g such that $(g \cdot v^+)_\lambda = 0$ for all $\lambda \in \Gamma$. Set $A := U(\Phi^+, I) \cdot U(\Phi^-, I) \cdot B \cdot \text{EP}_s(R, I)$.

Let g be an element of $E(\Delta_r, R, I)$. Applying Lemma 3.10 to the subsystem Δ_r , we find $x \in U(\Delta_r^+, I)$ and $y \in U(\Delta_r^-, I)$ such that $yx \cdot g \in B$. Consequently, this shows that $A = A_{rs}$, indeed:

$$U(\Sigma_r^+, I) \cdot U(\Sigma_r^-, I) \cdot g = U(\Sigma_r^+, I) x^{-1} \cdot U(\Sigma_r^-, I) y^{-1} (yxg) \subseteq U(\Phi^+, I) \cdot U(\Phi^-, I) \cdot B.$$

Notice that by the definition of Γ and Lemma 2.3 for any $s \in I$, $g \in B$ one has $x_{-\alpha_r}(s) \cdot g \cdot v^+ = g \cdot v^+$. Consequently, one has

$$X_{-\alpha_r}(I)^B \subseteq U(\Phi^-, I) \cap \text{Stab}(v^+) \subseteq U(\Delta_s^-, I) \subseteq \text{EP}_s(R, I),$$

which implies the following inclusion:

$$\begin{aligned} X_{\alpha_r}(I) \cdot X_{-\alpha_r}(I) \cdot B \cdot \text{EP}_s(R, I) &\subseteq X_{\alpha_r}(I) \cdot B \cdot \text{EP}_s(R, I) \cdot \text{EP}_s(R, I) \subseteq \\ &\subseteq B \cdot \text{U}(\Sigma_r^+, I) \cdot \text{EP}_s(R, I) = B \cdot \text{EP}_s(R, I). \end{aligned}$$

Together with the third statement of Lemma 4.5 this shows that

$$A = \text{U}(\Phi^+ \setminus \{\alpha_r\}, I) \cdot \text{U}(\Phi^-, I) \cdot B \cdot \text{EP}_s(R, I).$$

Finally, since $[B, X_{-\alpha_r}(R)] \subseteq \text{U}(\Sigma_r^-, R) \cap \text{E}(\Phi, R, I) = \text{U}(\Sigma_r^-, I)$, we obtain the assertion of the lemma. Indeed,

$$A^{X_{-\alpha_r}(R)} = \text{U}(\Phi^+, I) \cdot \text{U}(\Phi^-, I) \cdot B^{X_{-\alpha_r}(R)} \cdot \text{EP}_s(R, I) = A. \quad \square$$

Lemma 4.7. *Assume that one of the following holds:*

- (1) $\Phi = \mathbb{C}_\ell$ and $\text{sr}(I) \leq \ell - 1$;
- (2) $\Phi = \mathbb{F}_4$ and $\text{asr}(I) \leq 3$.

Then one has $X_{-\alpha_s}(R) \subseteq N_{rs}$.

Proof. Consider the subset $C \subseteq \text{EP}_s(R, I)$, consisting of the elements satisfying the following condition:

- CASE $\Phi = \mathbb{C}_\ell$. Matrix entries $(g_{i,2})$, $i = 2, \dots, \ell$ form an I -unimodular column of height $\ell - 1$.
- CASE $\Phi = \mathbb{F}_4$. Matrix entries $(g_{\lambda,\lambda}, \dots, g_{\lambda,\lambda-\alpha_3-\alpha_2-\alpha_1})$, where $\lambda = \varpi_4 - \alpha_4$ (see [16, Fig. 26]), form an I -unimodular column of height 4.

Set $A' = \text{EP}_\ell(R, I) \cdot \text{U}(\Sigma_s^- \cap \Sigma_r^-, I) \cdot C$. By Lemma 3.8.(i) (in the case $\Phi = \mathbb{C}_\ell$) or Corollary 3.9 (in the case $\Phi = \mathbb{F}_4$), applied to the subgroup $\text{G}(\Delta_s, R, I)$, we find for every $g \in \text{EP}_s(R, I)$ an element $x \in \text{U}(\Sigma_r^+ \cap \Delta_s, I)$ such that $xg \in C$. Notice that one immediately gets the equality $A_{rs} = A'$ from this. Indeed, for $g \in \text{EP}_s(R, I)$ one has

$$\text{EP}_r(R, I) \cdot \text{U}(\Sigma_s^- \cap \Sigma_r^-, I) \cdot g \subseteq \text{EP}_r(R, I)x^{-1} \cdot \text{U}(\Sigma_s^-, I) \cdot xg \subseteq A'.$$

By the very definition of C , for every $g \in C$ one can choose $y \in \text{U}(\Sigma_s^+ \cap \Delta_r, I)$ such that $(y \cdot g)_{\varpi_s, \varpi_s - \alpha_s} = 0$. Consequently, for every $g \in C$ one has

$$\begin{aligned} \text{EP}_r(R, I) \cdot \text{U}(\Sigma_s^- \cap \Sigma_r^-, I) \cdot g &\subseteq \text{EP}_r(R, I)y^{-1} \cdot \text{U}(\Sigma_r^- \cap \Sigma_s^-, I)y \cdot yg \subseteq \\ &\subseteq \text{EP}_r(R, I) \cdot \text{U}(\Sigma_r^-, I) \cdot yg. \end{aligned}$$

Notice that the matrix entry $(yg)_{\varpi_s, \varpi_s}$ is invertible. From the choice of y it follows that for every $\xi \in R$ the element $g_1 := (yg)^{x_{-\alpha_s}(\xi)}$ satisfies the assumptions of Lemma 2.5 and therefore can be rewritten as $g_1 = uh$ for some $u \in \text{U}(\Sigma_s^-, I)$, $h \in \text{EP}_1(R, I)$. Consequently, one has

$$\begin{aligned} A_{rs}^{X_{-\alpha_s}(R)} &\subseteq \text{EP}_r(R, I)^{X_{-\alpha_s}(R)} \cdot \text{U}(\Sigma_r^-, I)^{X_{-\alpha_s}(R)} \cdot \text{U}(\Sigma_s^-, I) \cdot \text{EP}_s(R, I) \subseteq \\ &\subseteq \text{EP}_\ell(R, I) \cdot \text{U}(\Phi^-, I) \cdot \text{EP}_s(R, I) \subseteq A_{rs}, \end{aligned}$$

as claimed. \square

5. APPLICATIONS

5.1. Bounded generation. We now give an application of the parabolic factorizations to the problem of bounded generation.

Lemma 5.1. *In the assumptions of Theorem 1 the width of $E(\Phi, R, I)$ with respect to $\mathcal{Z}(\Pi)$ does not exceed $3|\Phi^+| + 2\text{rk } \Phi - 1$.*

Proof. Take an element $g \in E(\Phi, R, I)$ and decompose it into $g = u_1 h v_2 u_3$, where $h \in H(\Phi, R, I)$, $u_1, u_3 \in U(\Phi, I)$, $v_2 \in U(\Phi^-, I)$. Write $h = \prod_{i=1}^{\ell} h_{\alpha_i}(\varepsilon_i)$, $\varepsilon_i \in 1 + I$. Each $h_{\alpha_i}(\varepsilon_i)$ decomposes into $h_{\alpha_i}(\varepsilon_i) = x_{\alpha_i}(\varepsilon_i) z_{-\alpha_i}(\varepsilon_i) x_{-\alpha_i}(\varepsilon_i)$ (see (2.8)), and since the torus normalizes each of $X_{\alpha}(I)$ (see formula (2.6)), we have a decomposition

$$g \in U(\Phi, I) \cdot \prod_{i=1}^{\ell} (x_{\alpha_i}(\varepsilon_i) z_{-\alpha_i}(\varepsilon_i) x_{-\alpha_i}(\varepsilon_i)) \cdot U^-(\Phi, I) U(\Phi, I),$$

and the estimate follows. \square

The following lemma is a corollary of Theorems 5.7 and 5.8 of [10].

Lemma 5.2. *Let p be a rational prime, let c, d be a pair of coprime integers such that $p \perp d$. Then under the assumption of the Generalized Riemann Hypothesis there exist infinitely many primes $q \equiv c \pmod{d}$ such that p is a primitive root modulo q .*

The following lemma is a relative version of [33, Lemma 6] (see also [34]):

Lemma 5.3. *Set $R = \mathbb{Z}[1/p]$ and let I be an ideal of R . Under the assumption of the GRH the width of $\text{SL}(2, R, I)$ with respect to the generating set*

$$\mathcal{Z}(\{-\alpha_1\}) = X_{12}(I) \cup X_{21}(I) \cup \{z_{21}(s, \xi) \mid s \in I, \xi \in R\}$$

does not exceed 6.

Proof. Clearly, I is a principal ideal generated by some integer $m \in \mathbb{Z}$ not divisible by p . Let g be an element of $\text{SL}(2, R, I)$. Write

$$g = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, \text{ for } x = p^{\alpha}a, z = p^{\beta}bm, \text{ where } a, b, \alpha, \beta \in \mathbb{Z}, p \nmid a, b.$$

CASE 1: $\alpha \geq \beta$. Since $p^{\alpha-\beta}a \perp bm^2$ and $p \perp bm^2$, there exist infinitely many rational primes q of the form $p^{\alpha-\beta}a + bm^2k$, such that p is a primitive root modulo q . We may assume that q is prime to b . Write

$$g_1 = x_{12}(mk) \cdot g = \begin{pmatrix} p^{\beta}q & * \\ p^{\beta}bm & * \end{pmatrix}.$$

There exists $u \geq 1$ such that $p^u \equiv b \pmod{q}$, say $p^u = b + lq$. Then

$$g_2 = x_{21}(ml) \cdot g_1 = \begin{pmatrix} p^{\beta}q & * \\ mp^{\beta+u} & * \end{pmatrix}.$$

Since $g_2 \equiv 1 \pmod{m}$, we can write $p^\beta q = 1 + cm$ for some c . Now set

$$\begin{aligned} g_3 &= x_{12} \left(\frac{-c}{p^{\beta+u}} \right) \cdot g_2 = \begin{pmatrix} 1 & * \\ mp^{\beta+u} & * \end{pmatrix}, \\ g_4 &= x_{21} (-mp^{\beta+u}) \cdot g_3 = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}, \\ g_5 &= x_{12} \left(\frac{c}{p^{\beta+u}} \right) \cdot g_4 = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}. \end{aligned}$$

Notice that $g_5 = z_{21} (-mp^{\beta+u}, c/p^{\beta+u}) \cdot g_2$ hence $g = x_{12} \cdot x_{21} \cdot z_{21} \cdot x_{12}$ and the length of g does not exceed 4.

CASE 2: $\alpha < \beta$. Since $\mathbb{Z}[1/p]/I$ is finite, there exists $k > 0$ such that $p^k \equiv 1 \pmod{I}$. One can choose $k > \beta - \alpha$. Then $k + \alpha > -k + \beta$ and

$$h_{12}(p^k) \cdot g = \begin{pmatrix} p^k & 0 \\ 0 & p^{-k} \end{pmatrix} \begin{pmatrix} p^\alpha a & * \\ p^\beta bm & * \end{pmatrix} = \begin{pmatrix} p^{k+\alpha} a & * \\ p^{-k+\beta} bm & * \end{pmatrix}.$$

We find ourselves in the situation of the previous case, therefore, we can write $g = h_{12} \cdot x_{12} \cdot x_{21} \cdot z_{21} \cdot x_{12}$. Finally, expressing $h = x_{21} \cdot z_{21} \cdot x_{12}$ as in (2.8), we get that $g = x_{21} \cdot z_{21} \cdot x_{12} \cdot x_{21} \cdot z_{21} \cdot x_{12}$. \square

For the rest of this subsection k denotes a global field. We assume that there is some finite set of places S chosen on k . Let \mathcal{O}_S be a Dedekind ring of arithmetic type defined by S and let I be an ideal of \mathcal{O}_S .

Lemma 5.4. *Let Φ be an irreducible classical root system of rank $\ell \geq 2$. If k has a real embedding, then $G(\Phi, \mathcal{O}_S, I)$ has finite width with respect to the generating set $\mathcal{Z}(\Sigma_\ell)$.*

Proof. First of all, notice that $\text{asr}(I) \leq \text{asr}(\mathcal{O}_S) \leq 2$. By Corollary 4.3 we can present any element of $G = G(\Phi, \mathcal{O}_S, I)$ as a product of a finite number of generators from $\mathcal{Z}(\Sigma_\ell)$ and one element of $G_0 = G(\{\alpha_\ell, -\alpha_\ell\}, \mathcal{O}_S, I) \cong \text{SL}(2, \mathcal{O}_S, I)$. Consequently, to prove the statement of the lemma it suffices to express every element $g = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in G_0$ as a product of a finite number of generators contained in some rank 2 subgroup of G containing G_0 .

From $\det(g) = 1$ we conclude that $a + d = bc - ad \in I^2$. Recall that the Vaserstein's congruence subgroup is defined as

$$G(I, I) = \left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in \text{SL}(2, \mathcal{O}_S) \mid a, d \in I^2, b, c \in I \right\}.$$

Notice that $g_1 = g \cdot z_{21}(a, 1)$ is contained in $G(I, I)$, indeed,

$$\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \cdot \begin{pmatrix} 1-a & -a \\ a & 1+a \end{pmatrix} = \begin{pmatrix} 1+ba-a^2 & b-a-ba-a^2 \\ c+a+ad-ac & 1+bc-ac \end{pmatrix} \in G(I, I).$$

For any matrix $g' = \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} \in G(I, I)$ the matrix $x_{21}(-c) \cdot g' \cdot x_{12}(-b)$ lies in $\text{SL}(2, \mathcal{O}_S, I^2)$.

By Lemma 2.4 the group $E(\Phi, \mathcal{O}_S, I^2)$ is contained in $E(\Phi, I)$ for any root system $\Phi \neq C_\ell$ of rank ≥ 2 . Notice that under the assumptions of the lemma it is known that $E(\Phi, I)$ has finite width with respect to \mathcal{X} , see [23, Theorem 3.3].

It remains to consider the case $\Phi = C_\ell$. First of all, notice that $2abc - abd \in II^{\mathbb{Q}}$, indeed,

$$\det(g_1) = a^3d - 3a^2bc + a^2bd + ab^2c + a^3 + a^2b + a^2d + 2abc - abd + 1.$$

This means that

$$g_2 = x_{21}(-a - c) \cdot g_1 \cdot x_{12}(a - b) \equiv \begin{pmatrix} 1 + ab - a^2 & -ab - a^2 \\ ad - ac - abc & 1 - ab + a^2 \end{pmatrix} \pmod{II^{\mathbb{Q}}}.$$

Now for $g_3 = g_2 \cdot z_{12}(a^2 - ab, 1)$ we have that

$$g_3 \equiv \begin{pmatrix} 1 & -2ab \\ -abc - a^2 + ab - ac + ad & 1 \end{pmatrix} \pmod{II^{\mathbb{Q}}},$$

$$g_4 = x_{12}(2ab) \cdot g_3 \equiv x_{21}(-abc - a^2 + ab - ac + ad) \pmod{II^{\mathbb{Q}}}.$$

Thus $g_4 \cdot x_{21}(*) \in \mathrm{SL}(2, \mathcal{O}_S, II^{\mathbb{Q}})$ is contained in $E(\mathbb{C}_\ell, I)$ by Lemma 2.4 and therefore can be expressed as a bounded product of x_α . \square

Proof of Theorem 3. The second assertion of the theorem is contained in Lemma 5.1. The first and the third assertions follow from Lemmas 5.3 and 5.4. \square

5.2. Subsystem factorizations. Consider the decreasing chain Φ_k , $k = 1, \dots, \lfloor \ell/2 \rfloor$ of root subsystems of $\Phi = D_\ell$ defined as follows. If $2k \neq \ell$, let Φ_k be the subsystem of Φ , spanned by the fundamental roots $\alpha_{2k-1}, \dots, \alpha_\ell$. Clearly, such Φ_k has type $D_{\ell-2k+2}$. In the remaining case $2k = \ell$ set $\Phi_k = \langle \alpha_\ell \rangle \cong A_1$. Now let β_k be the maximal root of Φ_k , i.e. $\beta_k = \alpha_{\max}(\Phi_k)$, $k = 1, \dots, \lfloor \ell/2 \rfloor$. Denote by B the set of all β_k . From the definition it is clear that the elements of B are mutually orthogonal to each other. The roots β_k can also be defined by explicit formulae:

$$\begin{aligned} \beta_k &= \alpha_{2k-1} + 2\alpha_{2k} + \dots + 2\alpha_{\ell-2} + \alpha_{\ell-1} + \alpha_\ell, \text{ for } k = 1, \dots, \lfloor \ell/2 \rfloor - 1, \\ \beta_{\lfloor \ell/2 \rfloor} &= \alpha_{\ell-2} + \alpha_{\ell-1} + \alpha_\ell, \text{ if } \ell \text{ is odd,} \\ \beta_{\lfloor \ell/2 \rfloor} &= \alpha_\ell, \text{ if } \ell \text{ is even.} \end{aligned}$$

Lemma 5.5. *There exists an element $w \in W(D_\ell)$ such that $w(B) \subseteq \Delta_\ell^+$.*

Proof. CASE $\ell = 4$. Set $w = \sigma_{\alpha_1 + \alpha_2} \circ \sigma_{\alpha_2 + \alpha_4}$. Straightforward computation shows that

$$\begin{aligned} w(\beta_1) &= w(\alpha_{\max}) = \sigma_{\alpha_1 + \alpha_2}(\alpha_1 + \alpha_2 + \alpha_3) = \alpha_3, \\ w(\beta_2) &= w(\alpha_4) = \sigma_{\alpha_1 + \alpha_2}(-\alpha_2) = \alpha_1, \end{aligned}$$

which implies the assertion of the lemma.

CASE $\ell \geq 5$. Recall from [5, Table 9] that for odd (resp. even) ℓ all maximal subsystems of type $A_1 + \dots + A_1 + D_3$ (resp. $A_1 + \dots + A_1 + D_4$) are conjugate under the action of $W(\Phi)$. Consequently, we can find $w \in W(\Phi)$ such that $w(\beta_k) = \alpha_{2k-1}$ for $k < \lfloor \ell/2 \rfloor$ (resp. $k < \lfloor \ell/2 \rfloor - 1$). Now using transitivity of the action of $W(D_3)$ on the roots (resp. by the same argument as in the case $\ell = 4$) we can move the remaining root $\beta_{\lfloor \ell/2 \rfloor}$ (resp. the remaining 2 roots $\beta_{\lfloor \ell/2 \rfloor - 1}, \beta_{\lfloor \ell/2 \rfloor}$) to $\alpha_{\ell-1}$ (resp. to $\alpha_{\ell-3}, \alpha_{\ell-1}$) while fixing all the other β_k . \square

The following lemma is an analogue of Proposition 1 of [15].

Lemma 5.6. *Let $\Phi = D_\ell$, $\ell \geq 2$ and let I be an ideal of a commutative ring R . There exist an element $y \in E(\Phi, R)$ and an element $w \in \widetilde{W}(\Phi)$ such that*

$$U(\Sigma_\ell^+, I) \subset [U(\Delta_\ell^-, I), y] \cdot {}^w U(\Delta_\ell^+, I).$$

Proof. Since $U(\Sigma_\ell^+, I)$ is abelian, we can decompose it as $U(\Sigma_\ell^+, I) = U(\Sigma_\ell^+ \setminus B, I) \cdot U(B, I)$. Set $y = \prod_{\beta \in B} x_\beta(1)$. We will now show by induction on ℓ that

$$(5.1) \quad U(\Sigma_\ell^+ \setminus B, I) \subset [U(\Delta_\ell^-, I), y] \cdot U(B, I).$$

The induction base in the cases $\ell = 2, 3$ is trivial.

Notice that β_1 is the only root of Φ satisfying $m_2(\beta_1) = 2$, therefore the commutator formula (2.2) implies

$$[U(\Delta_2^-, I), x_{\beta_1}(1)] = 1.$$

There is no root of the form $\gamma = \alpha + \beta$ with $\alpha \in \Sigma_2^- \cap \Delta_\ell$ and $\beta \in B \setminus \{\beta_1\}$, because such a root γ must satisfy $m_2(\gamma) = -1$ and $m_\ell(\gamma) = 1$. Thus (2.2) gives

$$\left[U(\Sigma_2^- \cap \Delta_\ell, I), \prod_{i \neq 1} x_{\beta_i}(1) \right] = 1.$$

Since $B \setminus \{\beta_1\} \subset \Sigma_\ell^+ \cap \Delta_2$, the above two identities imply

$$\begin{aligned} \left[U(\Sigma_2^- \cap \Delta_\ell, I) \cdot U(\Delta_{2,\ell}^-, I), x_{\beta_1}(1) \cdot \prod_{i \neq 1} x_{\beta_i}(1) \right] &\equiv \\ &\equiv [U(\Sigma_2^- \cap \Delta_\ell, I), x_{\beta_1}(1)] \bmod U(\Sigma_\ell^+ \cap \Delta_2, I). \end{aligned}$$

Take an element $u \in U(\Sigma_2^- \cap \Delta_\ell, I)$ and decompose it as $u = vw$, where $v \in U(\Sigma_1^- \cap \Sigma_2^- \cap \Delta_\ell, I)$ and $w \in U(\Sigma_2^- \cap \Delta_{1,\ell}, I)$. Using the identity

$$(5.2) \quad [ab, c] = {}^a[b, c] \cdot [a, c],$$

we can rewrite

$$[vw, x_{\beta_1}(1)] = {}^v[w, x_{\beta_1}(1)] \cdot [v, x_{\beta_1}(1)].$$

Since $U(\Sigma_1^- \cap \Sigma_2^- \cap \Delta_\ell, I)$ and $U(\Sigma_2^- \cap \Delta_{1,\ell}, I)$ are abelian, it is easy to see that

$$[v, x_{\beta_1}(1)] \in U(\Sigma_2^+ \cap \Sigma_\ell^+ \cap \Delta_1, I), \quad [w, x_{\beta_1}(1)] \in U((\Sigma_1^+ \cap \Sigma_\ell^+) \setminus \{\beta_1\}, I).$$

Every element of $U(\Sigma_2^+ \cap \Sigma_\ell^+ \cap \Delta_1, I)$ (resp. $U(\Sigma_1^+ \cap \Sigma_\ell^+ \setminus \{\beta_1\}, I)$) can be expressed as such a commutator for a suitable choice of v (resp. w). Indeed, set $v = x_\gamma(\xi_\gamma) \cdot v'$, $\gamma = -\alpha_1 - \alpha_2$, $v' \in U(\Sigma_1^- \cap \Sigma_2^- \cap \Delta_\ell \setminus \{\gamma\}, I)$. Using relation (5.2) and the fact that $X_\gamma(I)$ commutes with $U(\Sigma_2^+ \cap \Delta_1, I)$ we get that:

$$\begin{aligned} [v, x_{\beta_1}(1)] &= [x_\gamma(\xi_\gamma) \cdot v', x_{\beta_1}(1)] = {}^{x_\gamma(\xi_\gamma)}[v', x_{\beta_1}(1)] \cdot [x_\gamma(\xi_\gamma), x_{\beta_1}(1)] = \\ &= [v', x_{\beta_1}(1)] \cdot x_{\beta_1 - \alpha_1 - \alpha_2}(\xi_\gamma) = \dots = \prod_{\alpha \in \Sigma_1^- \cap \Sigma_2^- \cap \Delta_\ell} x_{\beta_1 + \alpha}(\xi_\alpha). \end{aligned}$$

It remains to note that $\Sigma_2^+ \cap \Sigma_\ell^+ \cap \Delta_1 = \beta_1 + \Sigma_1^- \cap \Sigma_2^- \cap \Delta_\ell$. The same argument works for $[w, x_{\beta_1}(1)]$. Direct calculation using the commutator formula shows that

$${}^v U(\Sigma_1^+ \cap \Sigma_\ell^+ \setminus \{\beta_1\}, I) \equiv U(\Sigma_1^+ \cap \Sigma_\ell^+ \setminus \{\beta_1\}, I) \bmod U(\Sigma_\ell^+ \cap \Delta_2, I).$$

Summing up the above arguments, we get that

$$[U(\Sigma_2^-, I) \cdot U(\Delta_{2,\ell}^-, I), y] \equiv U((\Sigma_{1,2}^+ \cap \Sigma_\ell^+) \setminus \{\beta_1\}) \bmod U(\Sigma_\ell^+ \cap \Delta_2, I),$$

hence the inclusion (5.1) follows from the induction hypothesis (applied to $\Delta_{1,2} \cong D_{\ell-2}$).

Finally, we have found $a \in U(\Sigma_\ell^+ \setminus B, I)$ and $b \in U(\Delta_\ell^-, I)$ such that

$$a \in [b, y] \cdot \prod_{\beta \in B} X_\beta \subset [U(\Delta_\ell^-, I), y] \cdot U(B, I).$$

Now the assertion of the lemma follows from Lemma 5.5. \square

Proof of Theorem 5. Set $L = E(\Delta_\ell, R, I) \leq E(D_\ell, R, I)$ and denote by σ the automorphism of $G(D_\ell, R)$ induced by the diagram automorphism of D_ℓ swapping α_ℓ and $\alpha_{\ell-1}$. By Theorem 2 one has

$$\begin{aligned} E(D_\ell, R, I) &= EP_\ell(R, I) \cdot U(\Sigma_{\ell-1}^- \cap \Sigma_\ell^-, I) \cdot EP_{\ell-1}(R, I) = \\ &= L \cdot U(\Sigma_\ell^+, I) \cdot U(\Sigma_{\ell-1}^- \cap \Sigma_\ell^-, I) \cdot (L \cdot U(\Sigma_\ell^+, I))^\sigma. \end{aligned}$$

Now using Lemma 5.6, one can find $y_1, y_2 \in G(D_\ell, R)$ and $w_1, w_2 \in \widetilde{W}(D_\ell)$ such that

$$\begin{aligned} L \cdot U(\Sigma_\ell^+, I) &\subset L \cdot U(\Delta_{\ell-1}^-, I) \cdot {}^{y_1}U(\Delta_{\ell-1}^-, I) \cdot {}^{w_1}U(\Delta_{\ell-1}^+, I), \\ U(\Sigma_{\ell-1}^- \cap \Sigma_\ell^-, I) &\subset U(\Delta_\ell^+, I) \cdot {}^{y_2}U(\Delta_\ell^+, I) \cdot {}^{w_2}U(\Delta_\ell^-, I). \end{aligned}$$

Thus $E(D_\ell, R, I)$ is a product of at most 9 conjugates of $L \cong E(A_{\ell-1}, R, I)$. \square

REFERENCES

- [1] E. Abe and K. Suzuki. “On normal subgroups of Chevalley groups over commutative rings”. *Tohoku Math. J.* Vol. 28, No. 2, (1976), pp. 185–198.
- [2] H. Azad, M. Barry, and G. Seitz. “On the structure of parabolic subgroups”. *Comm. Algebra* Vol. 18, No. 2, (1990), pp. 551–562.
- [3] H. Bass, J. Milnor, and J.-P. Serre. “Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)”. *Publ. Math. IHES* Vol. 33, No. 1, (1967), pp. 59–137.
- [4] M. Demazure. “Groupes réductifs; unicité des groupes épinglés”. In: *Structure des schémas en groupes réductifs*. Vol. 153. Lect. Notes Math. Springer Berlin Heidelberg, 1970, pp. 263–322.
- [5] E. B. Dynkin. “Semisimple subalgebras of semisimple Lie algebras”. *Amer. Math. Soc. Transl.* Vol. 6, (1957), pp. 111–244.
- [6] D. R. Estes and J. Ohm. “Stable range in commutative rings”. *J. Algebra* Vol. 7, No. 3, (1967), pp. 343–362.
- [7] F. Grunewald, J. Mennicke, and L. Vaserstein. “On the groups $SL_2(\mathbb{Z}[x])$ and $SL_2(k[x, y])$ ”. *Israel J. Math.* Vol. 86, No. 1, (1994), pp. 157–193.
- [8] U. Hadad. “On Kazhdan constants of finite index subgroups in $SL_n(\mathbb{Z})$ ”. *Int. J. Algebra Comput.* Vol. 22, No. 3, (2012), p. 1250026.
- [9] M. I. Krusemeyer. “Fundamental groups, algebraic K -theory, and a problem of Abhyankar”. *Invent. Math.* Vol. 19, No. 1, (1973), pp. 15–47.
- [10] H. W. Lenstra Jr., P. Stevenhagen, and P. Moree. “Character sums for primitive root densities”. *Math. Proc. Cambridge Phil. Soc.* Vol. 157, No. 3, (Nov. 2014), pp. 489–511.
- [11] M. Liebeck, N. Nikolov, and A. Shalev. “Groups of Lie type as products of SL_2 subgroups”. *J. Algebra* Vol. 326, No. 1, (2011), pp. 201–207.
- [12] B. A. Magurn, W. van der Kallen, and L. N. Vaserstein. “Absolute stable rank and Witt cancellation for noncommutative rings”. *Invent. Math.* Vol. 91, No. 3, (1988), pp. 525–542.
- [13] H. Matsumoto. “Sur les sous-groupes arithmétiques des groupes semi-simples déployés”. *Ann. Sci. ENS* Vol. 2, No. 1, (1969), pp. 1–62.
- [14] D. W. Morris. “Bounded generation of $SL(n, A)$ (after D. Carter, G. Keller, and E. Paige)”. *New York J. Math.* Vol. 13, (2007), pp. 383–421.
- [15] N. Nikolov. “A product decomposition for the classical quasisimple groups”. *J. Group Theory* Vol. 10, No. 1, (2007), pp. 43–53.

- [16] E. Plotkin, A. Semenov, and N. A. Vavilov. “Visual Basic Representations: An Atlas”. *Int. J. Algebra Comput.* Vol. 8, (1998), pp. 61–95.
- [17] A. Smolensky, B. Sury, and N. A. Vavilov. “Gauss decomposition for Chevalley groups, revisited”. *Int. J. Group Theory* Vol. 1, No. 1, (2012), pp. 3–16.
- [18] M. R. Stein. “Stability theorems for K_1 , K_2 and related functors modeled on Chevalley groups”. *Japan J. Math.* Vol. 4, No. 1, (1978), pp. 77–108.
- [19] A. Stepanov. “Elementary calculus in Chevalley groups over rings”. *J. Prime Res. Math.* Vol. 9, (2013), pp. 79–95.
- [20] A. A. Suslin and M. S. Tulenbaev. “Stabilization theorem for the Milnor K_2 -functor”. *J. Soviet Math.* Vol. 17, No. 2, (1981), pp. 1804–1819.
- [21] G. Taddei. “Normalité des groupes élémentaires dans les groupes de Chevalley sur un anneau”. In: *Applications of algebraic K-theory to algebraic geometry and number theory, Part II (Boulder, Colo., 1983)*. Vol. 55. Contemp. Math 2. 1986, pp. 693–710.
- [22] O. I. Tavgen. “Bounded generation of Chevalley groups over rings of algebraic S -integers”. *Math. USSR Izv.* Vol. 36, No. 1, (1991), pp. 101–128.
- [23] O. I. Tavgen. “Combinatorial methods in the theory of linear and arithmetic groups”. Habilitation thesis. Institute of Mathematics of Belarus Academy of Science, 1993.
- [24] J. Tits. “Systemes générateurs de groupes de congruence”. *C. R. Acad. Sci. Sér. A* Vol. 283, No. 9, (1976), pp. 693–695.
- [25] L. N. Vaserstein. “Bass’s first stable range condition”. *J. Pure Appl. Algebra* Vol. 34, No. 2, (1984), pp. 319–330.
- [26] L. N. Vaserstein. “On normal subgroups of Chevalley groups over commutative rings”. *Tohoku Math. J.* Vol. 38, No. 2, (1986), pp. 219–230.
- [27] L. N. Vaserstein. “On the stabilization of the general linear group over a ring”. *Math. USSR Sb.* Vol. 8, No. 3, (1969), pp. 405–424.
- [28] L. N. Vaserstein. “Stable rank of rings and dimensionality of topological spaces”. *Funct. Anal. Appl.* Vol. 5, No. 2, (1971), pp. 102–110.
- [29] L. N. Vaserstein and A. A. Suslin. “Serre’s problem on projective modules over polynomial rings, and algebraic K -theory”. *Math. USSR Izv.* Vol. 10, No. 5, (1976), pp. 993–1054.
- [30] N. A. Vavilov. “Can one see the signs of the structure constants?” *St. Petersburg Math. J.* Vol. 19, (2008), pp. 519–543.
- [31] N. A. Vavilov and E. I. Kovach. “ SL_2 -factorisations of Chevalley groups”. *J. Math. Sci.* Vol. 188, No. 5, (2013), pp. 483–489.
- [32] N. A. Vavilov and E. Plotkin. “Chevalley groups over commutative rings: I. Elementary calculations”. *Acta Appl. Math.* Vol. 45, No. 1, (1996), pp. 73–113.
- [33] N. A. Vavilov, A. V. Smolensky, and B. Sury. “Unitriangular factorizations of Chevalley groups”. *J. Math. Sci.* Vol. 183, No. 5, (2012), pp. 584–599.
- [34] M. Vsemirnov. “Short unitriangular factorizations of $SL_2(\mathbb{Z}[1/p])$ ”. *Quarterly J. Math.* Vol. 65, No. 1, (2013), pp. 279–290.

E-mail address: `sinchukss at yandex.ru`; `andrei.smolensky at gmail.com`